CGM webPRACTICE™
Self-Hosted
Hardware and Software
Full Requirements
April 12, 2023

CGMwebPRACTICE™

Fully Web-Based Practice Management Suite

Table of Contents

FULL SYSTEM REQUIREMENTS

CGM webPRACTICE customer configurations must meet the full system requirements as outlined in this document.

Server Specifications

When using CGM webPRACTICE in the self-hosted model, a server is required with hardware and software as outlined below.

Processor	Quad Core Intel® Xeon 3.0 GHz
Memory	8 GB RAM for Windows® 2016 12 GB RAM for Windows® 2019
Storage	Hardware RAID controller (RAID 5 or RAID 10 required) • Serial-attached-SCSI (SAS) drives • >/= 250 GB available disk space *after* OS install
Operating System	• Microsoft® Windows® Server 2016 • Microsoft® Windows® Server 2019 • Internet Information Services (IIS) installed onto drive C: with at least 20 GB **free** on the system partition. *Caution: Installation to Microsoft Windows Small Business Server (all editions) is not supported.*

Database Licensing (installed by CGM US)	***New Servers only for new clients or re-installations*** - CGM webPRACTICE runs on InterSystems' Cache technology. InterSystems offers several license versions depending on the CPU count of your server:
	Windows® 2016 & Windows® 2019
	       o 1 to 16 Cores – Entrée
	       o Unlimited Cores – Elite
	       o Unlimited Cores – Enterprise
	(Note that this is not the bare-metal CPU count, but the CPU count visible to the Operating System. Verify with your CGM US Sales Representative that you have the correct license version for your server.)

Disk Drives	DVD-ROM

Server Specifications (cont.)

Internet Browser	Google Chrome Microsoft® Edge®
Video	Minimum resolution of 1024 x 768, 16-bit color
Network Adaptor	1000 MBPS Gigabit Ethernet
UPS	1000 VA (auto shut down capable)
Firewall	HIPAA-compliant firewall (see www.hipaa.org or www.hhs.gov/ocr/hipaa, for more information) • FTP (Outgoing, Ports 20, 21) • SSL (Bidirectional, Port 443)
Backup Device	Capacity of backup device should be equal to, or larger than, the total disk space to ensure a complete system backup can be completed.
Antivirus Software	Business version anti-virus solution recommended
Additional Software and Hardware	• Adobe® Acrobat® Reader® v9.0 or higher • Microsoft® .NET Framework 2.0 and 3.5 with current Service Packs • Java 8 (LTS) JDK - (Azul Zulu 8.68.0.21-CA-win64 OpenJDK Runtime Environment build 1.8.0_362-b09) • Microsoft® Excel or LibreOffice recommended • Anti-spyware recommended • Monitor, keyboard, and mouse

Client Computer Specifications

CGM webPRACTICE requires the following hardware and software for each client computer (Desktop, Laptop, and Tablet).

Processor	Intel® Core™ 2 Duo; 2.66 GHz; 3 MB; 1066 MHz FSB or faster
Memory	8 GB RAM
Storage	80 GB formatted NTFS (SATA) – 40 GB Free after OS installation *Recommended*: 120 GB formatted NTFS (SATA)
Operating System	- Windows® 10 Pro or Enterprise - Windows® 11 Pro *Mac OS *Notes*: 1. *If running multiple CGM US applications, see the requirements for the other CGM applications for compatibility acceptance.* 2. **Mac OS® and hardware platform are only supported with Parallels installation. For detailed specifications for Mac computers, see page 8 of this document.*
Internet Browser	Google Chrome Microsoft® Edge®
Video	Minimum resolution of 1024 x 768, 32-bit color
Network Adapter	1000 MBPS Gigabit Ethernet
Remote Support	When CGM US support must gain access to a client computer to provide assistance, a one-time, secure connection is established with that computer—the client user initiates the session, and, after the session is finished and closed, access to that computer is no longer available.

Client Computer Specifications (cont.)

Antivirus Software	Business version anti-virus solution recommended
Additional Software and Hardware	• Adobe® Acrobat® Reader® v9.0 or higher • Microsoft® .NET Framework 2.0 and 3.5 with current Service Packs • Microsoft® Excel or LibreOffice recommended • Anti-spyware recommended • Monitor, keyboard, and mouse

Note: According to the terms of your support agreement, you must allow CGM US remote access to your system so that we can provide technical support. When remote assistance is required, a one-time, secure connection is established with the appropriate client computer—the client user initiates the session and, once the session is finished and closed, access to that computer is no longer available. Only authorized CGM US personnel may access your system; no CGM US personnel will open, modify, or view Patient Health Information (PHI) documents or data not directly pertaining to the repair, troubleshooting, or maintenance of your CGM webPRACTICE application.

Peripheral Specifications

Printers

Interface	USB/Network
CGM Recommended	Laser printer that is connected through the network and managed by the server

Peripheral Specifications (cont.)

Desktop Scanners

For daily scanning tasks, a desktop scanner is required.

Feed Type	Multi-sheet / single sided
Interface	USB/Network
Driver	TWAIN Compliant - **Note**: compliant is different from compatible.
CGM Recommended	- Fujitsu FI-7160 or FI-7260 (or comparable model) - Xerox® DocuMate™ 510 (or comparable model) - Panasonic KV-S1026C (or comparable model) Multi-function scanners and all-in-one fax/scanner/copier machines are not recommended. - EcoScan i4d or i6d Card Scanners (Insurance Cards, Drivers Licenses) **For CGM webSCAN™ and CGM Direct Scanning:** A Twain <u>compliant</u> scanner must be installed on each workstation that will be using CGM webSCAN. **Note**: compliant is different from compatible. **Recommended for CGM webSCAN™**: Inuvio EcoScan® i4d or i6d Card Scanners. The scanner must scan dual-sided and have auto-scan functionality that will automatically scan cards when inserted into scanner.

Internet Connection

CGM webPRACTICE products require a full- time, broadband Internet connection. The bandwidth speeds are the minimum recommendation for optimal experience with CGM webPRACTICE. If there is additional Internet traffic in the office, higher bandwidth may be required. For assistance in determining how much bandwidth your office may need to accommodate your scanning and image retrieval, please contact our Professional Services team at (855)-270-6700 Monday through Friday, 8 AM to 5 PM, Eastern Time.

Concurrent Users	Minimum Down
6 – 15	50 Mbps
16 – 50	75 Mbps
51 >	150 Mbps
The latency test average should not be > 70 ms.	

Notes: CGM US recognizes that you may want to use wireless network technology at your practice. Although this can provide an effective means of LAN communication, CGM US is unable to guarantee the reliability of this type of network infrastructure in conjunction with CGM webPRACTICE.

Mac Computer Specifications

CGM webPRACTICE requires the following hardware and software for each client computer (Desktop or MacBook).

Processor	Intel® Core™ 2 Duo; Core i3, Core i5, Core i7, Core i9, Intel Core M, or Xeon processor
Memory	8 GB RAM *Recommended*: 12 GB RAM (*for best performance*)
Storage	• 600 MB on the boot volume (Macintosh HD) for Parallels Desktop application installation • 100 GB additional disk space for virtual machines • SSD drive is recommended for better performance
Operating System	• macOS Mojave 10.14 • macOS High Sierra 10.13.6 or later • macOS Sierra 10.12.6 or later • OS X El Capitan 10.11.6 or later **Guest Operating System** • Windows® 10 Pro or Enterprise (Parallels required) • Windows® 11 Pro (Parallels required) *Notes*: 1. *If running multiple CGM US applications, see the requirements for the other CGM US applications for compatibility acceptance.*
Internet Browser	Google Chrome Microsoft® Edge®

Mac Computer Specifications (cont.)

Remote Support	When CGM US support must gain access to a client computer to provide assistance, a one-time, secure connection is established with that computer—the client user initiates the session, and, after the session is finished and closed, access to that computer is no longer available.
Antivirus Software	Business version anti-virus solution recommended
Additional Software and Hardware	• Adobe® Acrobat® Reader® v9.0 or higher • Microsoft® .NET Framework 2.0 and 3.5 with current Service Packs • Microsoft® Excel or LibreOffice recommended • Anti-spyware recommended

CGM WEBTOOLS™ TECHNICAL REQUIREMENTS

When using any of the CGM webTOOLS products, the following specifications are required. The most current version of the Technical Requirements for each CGM webTOOL can also be found in *CGM webPRACTICE Help* in the in the *Technical Documents* folder located within the *Knowledge Tree* folder.

Server Specifications

Only the technical requirements that are in addition to the CGM webPRACTICE System Requirements are listed below.

	Details
All CGM webTOOLS	Must meet the current CGM webPRACTICE System Requirements. Must be running on the most current version of CGM webPRACTICE. Your Project Manager can provide you with the current version number.
CGM webMOBILE™	**SSL Certificate:** Purchased or generated SSL certificate properly set up in Internet Information Services. 　**Note:** SSL purchase is not required. SSL Certificate can be created in Windows. **Port 443:** Port 443 needs to be opened on the firewall to allow access to the CGM webPRACTICE server.
CGM PRACTICE PORTAL™	**SSL Certificate:** Purchased SSL certificate properly set up in Internet Information Services on the Cache/CGM webPRACTICE server. 　**Notes:** In order to purchase and install the SSL certificate, you will need to first obtain a public IP address from your ISP and register a Domain name. SSL certificate can be purchased through GoDaddy, Network Solutions or the company of your choice. **Port 443:** Port 443 needs to be opened on the firewall to allow access to the CGM webPRACTICE server. **SMTP mail server:** A self-hosted SMTP mail server or standard SMTP ports need to be available. 　**Note:** SMTP TLS/SSL (sSMTP) is not supported at this time.
CGM webVERIFY™	Must be able to communicate with https://direct.emedixus.com.
CGM PinPoint™	Must be able to communicate with https://manageedocs.com.

Server Specifications (cont.)

	Details
CGM webPAY™ using TSYS	**Network Requirements** - The following sites must be accessible: t.broadpos.com - port 9020 must be configured for bidirectional communication. Ssl2.vitalps.net - port 5003 and port 443 must be configured for bidirectional communication. https://www.poslink.com/ws/process2.asmx must be accessible from the webPRACTICE server and the PAX devices. https://wpws.cgmus.com - must be accessible from the CGM webPRACTICE server.

Client Computer Specifications

Only the technical requirements that are in addition to the CGM webPRACTICE System Requirements for each client computer (Desktop, Laptop, and Tablet) are listed below.

	Details

CGM webMOBILE	**Web Browser Requirements for Mobile Devices**
	    Internet HTML: Standard language Version 3.2 or newer.
	    Other: JavaScript
	        Cascading Style Sheet (CSS) to view webMOBILE as designed. (CSS2.0 compliant recommended.)
	Mobile Devices – Supported OS
	    Windows Phone 7 or newer using Internet Explorer v7 or newer.
	    Apple iPhone v3 or newer using Safari
	    Android using Google Chrome
	    Blackberry 7250 (v4.1+)
	      Note: The appearance of webMOBILE on Blackberry devices is more basic due to the limitations of the Blackberry browser.
	    **Touchscreen devices are recommended for optimal performance.

CGM webSCAN™	**Scanner:** A Twain <u>compliant</u> scanner must be installed on each workstation that will be using CGM webSCAN. **Note**: compliant is different from compatible. **Recommended**: Inuvio EcoScan® i4d or i6d Card Scanners. The scanner must scan dual-sided and have auto-scan functionality that will automatically scan cards when inserted into scanner.
CGM Direct Scanning	**Scanner:** A Twain <u>compliant</u> scanner must be installed on each workstation that will be using CGM webSCAN. **Note**: compliant is different from compatible.

CGM PinPoint™	**Internet Browser**
	To connect to CGM PinPoint from within CGM webPRACTICE:
	Google® Chrome®
	Microsoft® Edge®
	
	To connect to CGM PinPoint directly:
	    Google® Chrome® - latest version
	    Microsoft® Edge® - latest version

Client Computer Specifications (cont.)

CGM webPAY™ using TSYS	**Network Requirements:** t.broadpos.com - port 9020 must be configured for bidirectional communication. Ssl2.vitalps.net - port 5003 and port 443 must be configured for bidirectional communication. https://www.poslink.com/ws/process2.asmx must be accessible from the webPRACTICE server and the PAX devices https://wpws.cgmus.com - must be accessible from the CGM webPRACTICE workstation. https://gateway.transit-pass.com - allows 'New card -manual entry' function.

TECHNICAL BACKUP INFORMATION

This information describes the files and directories, which must be backed up to ensure the ability to completely restore a CGM webPRACTICE system from backup in the event of a system failure, re-imaging, or hardware upgrade.

Completion of a backup includes verification of the backup completion and integrity, along with the periodic verification that the backup can be restored.

Full System Backup

A full system backup is a complete backup of all files on the system. This includes the operating system (e.g. Windows), the application (e.g. CGM webPRACTICE), and the data. Having a full system backup allows you to restore the system to working order in the shortest time possible since the operating system, data, and all programs are saved. A full system backup includes all files on all drives, local and networked (SAN, NAS, NFS, SAMBA, etc.), attached to the system.

Data Backup

A data backup stores the data files on the system which are changed regularly. Unlike the full system backup, the data backup does not back up the program files or the operating system. The data backup requires the existence of a full system backup or a complete reinstallation of the operating system and all associated programs to return the CGM webPRACTICE system to functionality.

A *Data Backup* must be completed daily.
- The database must be stopped before the backup is completed with the following **command:** {Cache installation drive}:\cachesys\bin\css stop cache
- After the backup has completed, the Cache database must be restarted with the following command**:** {Cache installation drive}:\cachesys\bin\css start cache
- The following directories must be backed up daily to ensure that your system is adequately protected. All files and directories below the listed directory must be backed up daily:

Location	Contents
{Cache installation drive}:\CacheSys	Cache Database, and configuration
{Installation drive}:\PermImages	EOB Scan images
{Installation drive}:\Transcription	Transcriptions
{Installation drive}:\CacheWeb	Required Cache files
{Installation drive}:\Remits	Electronic EOB (Insurance carriers)
{Installation drive}:\Reports	Confirmation reports for claims
{Installation drive}:\Claims	Claim files
{Installation drive}:\stmts	Statements
{Installation drive}:\TempImages	Temporary Images to be linked
{Installation drive}:\Program Files\Intellicus	CGM webREPORTS™ data

PRE-INSTALLATION REQUIREMENTS WORKSHEET

CGM webPRACTICE Server Details

Server Name: (as reported by hostname command)	
Fully Qualified Domain Name:	
Server/Domain Administrator Username (You can designate a different login with administrative privileges other than Administrator.)	
Server/Domain Administrator Password:	
Hard Drive Capacity GB:	
Memory Installed GB:	
Windows Version: (including Standard or Enterprise and service pack)	
Drive letter where CGM webPRACTICE should be installed:	
Processor Type and Clock Speed:	
Number of Processors as interpreted by Windows System Information: (For example, a single Dual-Core processor would be 2 processors)	
Is a proxy server set up on your network?	☐ Yes ☐ No IP Address_____ Port_____

SYSTEM REQUIREMENTS COMPLIANCE

By signing below, Customer agrees to maintain the above-mentioned software and hardware at its business to interact efficiently with the CompuGroup Medical US application CGM webPRACTICE.

CUSTOMER

Signature: _____

Printed Name: _____

Title: _____

Dated: _____