AMS System Specifications for Large Offices (6+ Computers)

American Medical Software runs on both 32 bit and 64 bit Windows operating systems. Speakers and/or headphones are required to hear audio from videos.

Additional products from Pervasive Software are necessary prior to installation of the AMS software. Version 10.30 or higher of Pervasive is the required minimum. Offices with 6 or more computers require the Pervasive Client/Server Engine. Pervasive products are available to AMS clients at a discount from Goldstar Software. Contact Bill Bach or Mary Jo Van Simpa at 708-647-7665 or sales@goldstarsoftware.com. Helpful hints for installing and using the AMS system with Pervasive PSQL are available at http://www.goldstarsoftware.com/apps_ams.asp.

Due to staggering number of additional SNOMED codes associated with ICD-10, all **Electronic Medical Records systems** are advised to meet the **"Recommended"** hardware specifications located below. Failure to do so may result in poor system performance and extremely long load times when searching the SNOMED database.

Minimum Requirements

The following requirements are the minimum system requirements for running the AMS software. Minimum system requirements are defined as: If the user configures their system using the minimum specifications for their specific requirements (users, remote sessions), under a full load, the software should continue to work in an acceptable manner on any given workstation. For example, if the maximum number of users are running normal day to day operations, a user in the software should still expect to receive a response from a patient search in less than four seconds. Of course, choosing hardware with much faster computing power will improve the performance of the software!

Recommended

These are the recommended specifications, not the minimum. Anything below these recommended specifications could result in poor system performance that cannot be "fixed" by AMS in any way due to poor hardware. As time goes on your AMS data size will continue to grow. With this in mind, you should increase your hardware's power accordingly in order to handle the higher demand required for processing larger volumes of information.

Dedicated File Server*	Minimum Requirements	Recommended
Operating System	Windows Server 2008 or Windows Server 2012.	Microsoft 64-bit Windows Server 2008 or Windows Server 2012. Other Windows operating systems are not recommended. Operating systems not supported by Microsoft are not supported by AMS due to Microsoft support termination.
Database Server	Pervasive PSQL v10.30 64-bit Server Engine	Pervasive PSQL v11.30 64-bit Server Engine
Screen Resolution	1024 x 768 resolution at 16-bit color depth or higher	1024 x 768 resolution at 16-bit color depth or higher
Optical Drive	16x DVD-ROM or better	32x DVD-ROM or better
Date Format	Computer MUST use US Standard MM/DD/YYYY date format.	Computer MUST use US Standard MM/DD/YYYY date format.
Language	Windows language MUST be set to English (U.S.)	Windows language MUST be set to English (U.S.)
6-20 Users:		
Processor	Intel Core 2 Duo E8500 or higher	Intel Core i7-3930K 3.2GHz LGA 2011 130W Six-Core Desktop Processor equivalent or higher
Memory	8 GB RAM	16 GB DDR3 RAM or higher
Hard Drive	40 GB of available hard drive space. 200+ GB of free hard drive space for the Electronic Medical Records Scanner Interface, as image files will take up considerably more disk space. *(Multiple Drives in Raid 5 configuration is recommended)*	1 TB of free hard drive space or higher *(Multiple Drives in Raid 5 configuration is recommended)*
20+ Users:		
Processor	Intel Core 2 Duo E8500 or higher	2xIntel Xeon E5-2430 2.2GHz 15MB L3 Cache LGA 1356 95W Six-Core Server Processor equivalent or higher in dual processor configuration
Memory	8 GB RAM	32 GB DDR3 RAM or higher

Hard Drive	40 GB of available hard drive space. 200+ GB of free hard drive space for the Electronic Medical Records Scanner Interface, as image files will take up considerably more disk space. *(Multiple Drives in Raid 5 configuration is recommended)*	2 TB of free hard drive space or higher *(Multiple Drives in Raid 5 configuration is recommended)*

Workstation

Operating System	Microsoft® Windows 10, Windows 8, Windows 7, or Windows Vista (Service Pack 2)	Microsoft 64-bit Windows 10 Pro, 64-bit Windows 8 Pro, or Windows 7 Professional *(Windows 8 RT is NOT supported)*
Database Server	Pervasive PSQL v10.30 Workgroup Engine	Pervasive PSQL v11.30 32-bit Client Engine *(64-bit Pervasive Client Support in the future)*
Processor	Intel Celeron 440, AMD Athlon 64 3200+ or better (Dual Core will improve Performance)	Intel Core i5-3470 3.2GHz LGA 1155 77W Quad-Core Desktop Processor equivalent or higher
Memory	2 GB RAM	6 GB DDR3 RAM or higher
Hard Drive	8 GB Free disk space *(8 GB is all that AMS and Windows require to run. It is recommended, however, that hard drives of no smaller size than 40 GB be installed on all workstations)*	250 GB of free hard drive space or higher
Screen Resolution	1024 x 768 resolution at 16-bit color depth or higher	1024 x 768 resolution at 16-bit color depth or higher
Date Format	Computer MUST use US Standard MM/DD/YYYY date format.	Computer MUST use US Standard MM/DD/YYYY date format.
Language	Windows language MUST be set to English (U.S.)	Windows language MUST be set to English (U.S.)

Laptops and Tablet PCs

Laptops	Laptops MUST have the same requirements as shown above for workstations.	Laptops MUST have the same recommendations as shown above for workstations.
Tablet PCs	Tablet PC's should be using the Microsoft® Windows 8, Windows 7, XP or Vista Tablet PC Edition operating system. *(This excludes Windows 8 RT as it is NOT supported)*	Microsoft Windows 8 or Windows 7 Tablet PC Edition operating system. *(This excludes Windows 8 RT as it is NOT supported)*
Laptops/Tablet PC's as Server	Laptops/Tablets are not acceptable for use as a server computers.	Laptops/Tablets are not acceptable for use as a server computers.

Remote Connections*

Operating System	Windows Server 2008, Windows 2003 Terminal Services, Citrix Metaframe Presentation Server 4.0 or higher. 1 to 3 Thin Clients can use the same dedicated server. 4 or more Thin Clients should have a separate server for the Remote Connections (Thin Clients)	Windows Server 2008 Terminal Services, Citrix Metaframe Presentation Server 6.5 or higher. Up to 10 Thin Clients should be easily able to use the same dedicated server as is outlined above. 11 or more Thin Clients should have a separate server for the Remote Connections (Thin Clients)

11-30 Thin Clients:

Processor	Intel Core 2 Duo E8500 or higher	Intel Xeon E5-2430 2.2GHz 15MB L3 Cache LGA 1356 95W Six-Core Server Processor equivalent or higher
Memory	2 GB RAM	6 GB DDR3 RAM
Network Interface Card	Microsoft recommends Dual NIC (Network Interface Cards) cards placed on different subnets, 1 for the Thin Client connections and the other for communicating with the AMS dedicated server.	Microsoft recommends Dual NIC (Network Interface Cards) cards placed on different subnets, 1 for the Thin Client connections and the other for communicating with the AMS dedicated server.

30+ Thin Clients:

Additional Servers	Multiple Terminal Servers and Load Balancing – 1 Additional Server needed for every 30 users. (31-60 users = 2 server, 61-90 users = 3 servers, etc.)	Multiple Terminal Servers and Load Balancing – 1 Additional Server needed for every 30 users. (31-60 users = 2 server, 61-90 users = 3 servers, etc.)

Networking

Internet Protocol Suite	TCP/IP	TCP/IP
Network Interface Card	100 Mbps Network Interface Card capable of supporting full-duplex operation	100 Mbps Network Interface Card capable of supporting full-duplex operation *(Gigabit Ethernet should be considered for 30+ users)*
Network Permsions	All workstations must have Full Control NTFS permissions and Full Control share permissions to the AMS data folder.	All workstations must have Full Control NTFS permissions and Full Control share permissions to the AMS data folder.

Wireless

Routers	Administrators should choose only routers that have WPA2 encryption capabilities. WPA2 contains the necessary security to ensure PHI is not compromised (i.e. 256-bit AES encryption, SHA-1 hashing, password/key authentication). Furthermore, a proper diagnostic of the facility and coverage should be performed to ensure that the wireless connection is strong, stable, and uninterrupted throughout EVERY room of the office. Low-end routers for home use (typically found on generic store shelves) should be left for home. Consult your IT professional about higher quality routers for business use.	Administrators should choose only routers that have WPA2 encryption capabilities. WPA2 contains the necessary security to ensure PHI is not compromised (i.e. 256-bit AES encryption, SHA-1 hashing, password/key authentication). Furthermore, a proper diagnostic of the facility and coverage should be performed to ensure that the wireless connection is strong, stable, and uninterrupted throughout EVERY room of the office. Low-end routers for home use (typically found on generic store shelves) should be left for home. Consult your IT professional about higher quality routers for business use.

Peripherals

Printers	For the printing of statements and the various forms generated by the AMS software, the HP LaserJet 3000 or 4000 Series printers are recommended. Inkjet printers, non HP-HP LaserJet printers, dot matrix printers, and HP LaserJet 1000 Series printers are not supported.	For the printing of statements and the various forms generated by the AMS software, the HP LaserJet 3000 or 4000 Series printers are recommended. Inkjet printers, non HP-HP LaserJet printers, dot matrix printers, and HP LaserJet 1000 Series printers are not supported.
Internet Access	For Electronic Claims Processing and downloading AMS Updates, an internet connection is required. Broadband internet connections (specifically Cable) are recommended. DSL is acceptable but generally performs poorer than cable.	For Electronic Claims Processing and downloading AMS Updates, an internet connection is required. Broadband internet connections (specifically Cable) are recommended. DSL is acceptable but generally performs poorer than cable.
Scanners	The Electronic Medical Records scanning interface can acquire images directly from MOST TWAIN compliant scanners. However, scanners are typically set to scan/deposit images in to a predetermined folder destination that the scanner interface them imports from. In this case, almost any scanner is acceptable.	The Electronic Medical Records scanning interface can acquire images directly from MOST TWAIN compliant scanners. However, scanners are typically set to scan/deposit images in to a predetermined folder destination that the scanner interface them imports from. In this case, almost any scanner is acceptable.
Reserve Power Supply	Uninterruptible Power Supply (UPS) – AMS required our client's Information Technology (IT) professional to properly install and configure a UPS on the client's server computer which has an interface to that server computer which will, in the event of an extended power loss, start a shutdown sequence within Windows prior to a total power failure. As part of the Microsoft Windows shutdown sequence a stop command is sent to the Pervasive service running on the server which closes all active transactions to the database and gracefully end the Pervasive Database Engine. This will help prevent data corruption or loss due to AC power failure in addition to extending the life and reliability of the connected server hardware and operating system. Consult your IT professional to help determine the required runtime and capacity of the UPS to allow enough time to properly execute the shutdown procedure.	Uninterruptible Power Supply (UPS) – AMS required our client's Information Technology (IT) professional to properly install and configure a UPS on the client's server computer which has an interface to that server computer which will, in the event of an extended power loss, start a shutdown sequence within Windows prior to a total power failure. As part of the Microsoft Windows shutdown sequence a stop command is sent to the Pervasive service running on the server which closes all active transactions to the database and gracefully end the Pervasive Database Engine. This will help prevent data corruption or loss due to AC power failure in addition to extending the life and reliability of the connected server hardware and operating system. Consult your IT professional to help determine the required runtime and capacity of the UPS to allow enough time to properly execute the shutdown procedure.

Backups

| Backup Solutions | For backing up the AMS data files, USB Flash drives (also known as "thumb drives" or "memory sticks") are highly recommended due to their durability and versatility for use with the integrated AMS backup program. Tape Backups/Online backups are acceptable backup medias, however the proprietary backup software used by these devices is NOT directly supported by AMS and may require the assistance of whoever installed it in order to extract or retrieve backup data.

NOTE: Due to the limited life cycle and durability of CDs, DVDs, CD-RWs, and DVD-RWs, they are NOT recommended. External Hard Drives are more reliable but are also not recommended. | |

*Dedicated File Server

A Dedicated File Server is a computer that is not used by anyone. Its sole function is to ensure that the workstations can access their data efficiently. They are commonly equipped with redundancy, such as RAID 5, which is 3 or more disks acting as one by striping data across all drives, so that if a drive fails the server will continue to run without data loss.

*Privacy and Security with Remote Connections

HIPAA requires all Protected Healthcare Information (PHI) to be secured and protected from confidentiality failures when transferred over open networks, such as wireless LAN connections and the Internet. The AMS software alone does not protect against these failures, therefore great care should be made in selecting software and hardware to encrypt PHI and prevent against false nodes.

American Medical Software recommends that for remote connections you use Remote Desktop Protocol (RDP) through Windows Terminal Services. Although RDP does offer 128 bit RC4 encryption, this encryption method has been found to be easily compromised and is not recommended for the transmission of PHI. Administrators should, in addition, ensure that all data is transported through Internet Protocol Security (IPSec) packets to create a Virtual Private Network (VPN). Administrators must choose and implement VPN software and hardware that uses AES or 3DES for encryption as well as SHA-1 hashing to protect the integrity of the data.

It is also worth mentioning that RDP alone does not prevent against Man in the Middle Attacks (MITM). To ensure node authenticity, administrators must set up their VPN's to use privately pre-shared keys, passwords, or use TLS (Transport Layer Services) to assign digital signatures to client machines.

The following is an example of a recommended secure remote environment:

The American Medical Software programs are installed on a Windows Server 2008 that is also running the Pervasive database server and is acting as a Windows Terminal Server. The server is connected to the internet via a VPN router (configured with 3DES or AES encryption and set to use a SHA-1 authentication algorithm). A private key has been set up on the router and a static UP address (assigned by the Internet Service Provider).

A remote computer connects through a remote desktop program (built in to Windows). The remote desktop program connects to the IP address of the router via a VPN client software (provided by the VPN manufacturer). The client software is set up with the same key previously set up on the router. The VPN client software is also set up with the same type of encryption method (AES or 3DES) and authentication algorithm (SHA-1) to verify data integrity. Once the connection is established through the router, the RDP connects to the Terminal Server and a desktop is created for the user. All communications between the sites are secure from intrusion because they are all encrypted and encapsulated in the IPSec protocol.

Please Note: AMS does not support the implementation, configuration, maintenance, or training of computer hardware products. AMS will ONLY provide assistance with issues originating from or through its software products.