

American Dental Association
Revised Technical Report No. 1055

Computer Hardware and Software Guidelines for Dental Offices

ADA American
Dental
Association®

2016

ADA Documents
Document Sharing Hub

Copyright © 2016 American Dental Association. All rights reserved. Any form of reproduction is strictly prohibited without prior written permission.

REVISED AMERICAN DENTAL ASSOCIATION TECHNICAL REPORT NO. 1055 FOR COMPUTER HARDWARE AND SOFTWARE GUIDELINES FOR DENTAL OFFICES

The Council on Dental Practice of the American Dental Association has approved American Dental Association Technical Report No. 1055 for Computer Hardware and Software Guidelines for Dental Offices. Working Groups of the ADA Standards Committee on Dental Informatics (SCDI) formulate this and other specifications and technical reports for the application of information technology and other electronic technologies to dentistry's clinical and administrative operations. The ADA SCDI has representation from appropriate interests in the United States in the standardization of information technology and other electronic technologies used in dental practice. The ADA SCDI confirmed approval of ADA Technical Report No. 1055 on January 27, 2016.

The ADA Standards Committee on Dental Informatics thanks the members of Working Group 10.11 on Computer Hardware and Software Guidelines and the organizations with which they were affiliated at the time the technical report was developed:

Mohamed Harunani (chairman), Academy of General Dentistry, private practice, Rockford, IL;

Scott Benjamin, Advanced Integration and Mentoring, Inc., Hancock, NY

Richard Celko, UPMC Health Plan, Pittsburgh, PA;

Zachary Church, Henry Schein Practice Solutions, American Fork, UT;

Stephen Glenn, private practice, Tulsa, OK;

Sue Kochlefl, Aetna, Inc., Glen Ellyn, IL;

Mary Licking, private practice, Nashua, NH;

John Martin, Previser Corp., Mount Vernon, WA;

Jim McLees, National Association of Dental Laboratories, Kent, WA;

Napoleon Monroe, Dental Trade Alliance, Arlington, VA;

Terry O'Toole, Department of Veteran's Affairs, Washington, DC;

Jeff Peacock, Henry Schein, Melville, NY;

Craig Ratner, private practice, Staten Island, NY; and

Mike Selberis, Glidewell Laboratories, Newport Beach, CA.

REVISED AMERICAN DENTAL ASSOCIATION TECHNICAL REPORT NO. 1055 FOR COMPUTER HARDWARE AND SOFTWARE GUIDELINES FOR DENTAL OFFICES

EXECUTIVE SUMMARY

(This Executive Summary does not form a part Revised American Dental Association Technical Report No. 1055 for Computer Hardware and Software Guidelines for Dental Offices).

The mountains of information available from vendors and the media on choosing practice management hardware and software can be bewildering and difficult for dentist to sort through in an effort to select the right system for their practice. The ADA Standards Committee on Dental Informatics (SCDI) has a long history of providing members assistance in selecting the practice management software and hardware systems that meet their specific needs, beginning with the first SCDI technical report, ADA Technical Report No. 1004, *Clinical Software Performance for Dental Practice Software*, published in 1998. This was followed in 2002 by ADA Technical Report No. 1012, *Hardware Recommendations for Dental Information Systems*. In 2011, the two reports were combined and updated for the first edition of ADA Technical Report No. 1055, *Computer Hardware and Software Guidelines for Dental Offices*.

This new revision of ADA Technical Report No. 1055 has been revised and expanded to include the latest recommendations on clinical utilization and electronic patient communications with guidelines on EHR, data security and privacy. As in the prior editions, the purpose of this technical report is to outline the features of hardware and software for dental practice management systems, to suggest specific selection guidelines for their optimal utilization in dental offices. Questions to ask hardware and software vendors when considering new systems are another valuable feature of this report.

The report begins by advising dentists to first select the all the practice management software products that will be utilized and to compile all their operating requirements. Only then should the hardware specification be determined. The system that is eventually purchased should be based on the highest minimum requirements of all software that will be utilized.

For software recommendations, the report outlines both basic features that should be required and additional features that are optional for general practice management and clinical systems. Systems covered include financial management and claims submittals, scheduling, digital imaging and patient communications, including privacy and security guidelines.

Computer hardware can have varying combinations. They can be standalone computers or they can be connected by a network, which may or may not be connected to a local server. The report provides recommended specifications for each of the main elements of a workstation or server computer for a dental practice: CPU (central processing unit), OS (operating system), RAM (random access memory), display adapter, disk drives, backup and network interface. Then the necessary peripheral equipment is covered: monitor, printer, input device, video capture card and network hardware.

In purchasing hardware, a dentist needs to consider the total cost of ownership, which includes the initial cost, cost of consumables, supplies, service/support and warranties and number of users supported.

And finally, best security practices should be followed by ensuring all computer systems are behind an internet firewall and have current anti-virus and malware applications installed and set to update automatically. Office policy should prohibit unauthorized use of websites and internet access by staff that could infect computer systems and compromise patient information, i.e., access to unsafe sites or to sites not required to perform their daily job functions. In addition, there should be no public access to the office network. Should the dentist wish to provide internet access, a separate Wi Fi system should be installed in the office.

REVISED AMERICAN DENTAL ASSOCIATION TECHNICAL REPORT NO. 1055 FOR COMPUTER HARDWARE AND SOFTWARE GUIDELINES FOR DENTAL OFFICES

FOREWORD

(This foreword does not form a part of Revised American Dental Association Technical Report No. 1055 for Computer Hardware and Software Guidelines for Dental Offices).

This document revises American Dental Association Technical Report No. 1055 for Computer Hardware and Software Guidelines for Dental Offices that was accepted in 2010. The 2010 version combined and replaced two previously published reports: ADA Technical Report No. 1012-2002 for Computer Hardware Recommendations for Dental Offices and ADA Technical Report No. 1004-2004 for Computer Software Performance for Dental Practice Software. This report was updated in 2015.

In 1992, there was interest in the standardization of clinical information systems related to electronic technology in the dental environment. After evaluating current informatics activities, a Task Group of the ANSI Accredited Standards Committee MD156 (ASC MD156) was created by the ADA to initiate the development of technical reports, guidelines, and standards on electronic technologies used in dental practice. In 1999, the ADA established the ADA Standards Committee on Dental Informatics (SCDI). The ADA SCDI is currently the group that reviews and approves proposed American National Standards (ANSI approved) and technical reports developed by the standards committee's working groups. The ADA became an ANSI accredited standards organization in 2000.

The scope of the ADA SCDI is:

The ADA SCDI shall develop informatics standards, specifications, technical reports and guidelines and interact with other entities involved in the development of health informatics standards aimed at implementation across the dental profession.

REVISED AMERICAN DENTAL ASSOCIATION TECHNICAL REPORT NO. 1055 FOR COMPUTER HARDWARE AND SOFTWARE GUIDELINES FOR DENTAL OFFICES

1 SCOPE

The purpose of this technical report is to outline the features of hardware and software for dental practice management systems and propose guidelines for selection for their optimal utilization in dental offices.

2 HARDWARE

Computer hardware requirements for dental offices can vary widely due to the variety of use and the large array of devices available. The design of computer hardware, the materials used in their manufacture and the various attachments are constantly changing.

Due to the increased environmental concerns, it is important that the user check local codes and regulations before purchasing or upgrading equipment including the adoption of more environmentally friendly “green” technologies. Users must comply with the Federal Resource Conservation and Recovery Act (RCRA) as well as other federal, state and local regulations on disposal of equipment containing hazardous materials.

When purchasing devices that will be used in clinical settings, users should ensure that devices such as keyboards and other input devices can be either barrier protected or disinfected to avoid transmission of infectious organisms. Users may consider the use of voice activated devices and/or other “hands-free” approaches to enable aseptic use. See *ADA Technical Report No. 1006 for Infection Control for Dental Information Systems*.¹

Dental offices can be divided into three categories:

1. Dental offices using only practice management software, accounting, spreadsheet and/or word processing software;
2. Dental offices using patient and clinical management software;
3. Dental offices using patient and clinical management software with integrated technological products, such as digital radiography, etc., a true “paper-less” office.

The types of software applications used in dental offices range from simple accounting programs to highly sophisticated imaging and design systems for various dental services, products and procedures. Users should work closely with their suppliers to ensure compatibility between the various hardware and software in their practice. The system should be optimized to meet their current and future needs, keeping in mind the potential growth of the practice and innovation in the field.

These recommendations promote the use of off-the-shelf computer hardware and devices as opposed to proprietary, closed systems that will most likely increase cost of ownership over time. Purchasing industry standard hardware also allows the most freedom of choice in choosing both a supplier and service provider who will be able to maintain the computer hardware over its useful lifetime.

Having an IT consultant or technician is very helpful when designing or updating to a “paper-less” environment. Consideration should be given to the management of all the paper documents, whether that is storage of the documents in a hard copy format or scanning and storing them digitally. Redundancy, security and patient privacy laws also should be considered.

Best security practices should be followed by ensuring all computer systems are behind an internet firewall and have current anti-virus and malware applications installed and set to update automatically. Furthermore, it is recommended that a security policy be put into effect that limits unauthorized use of websites and internet access by staff that could infect computer systems and compromise patient information, i.e., access to unsafe sites or to sites not required to perform their daily job functions should be restricted and enforced by policy.

A glossary of technical terms is included at the end of this document.

NOTE (1): Please refer to the practice management software vendor first to determine the hardware specification. The system that is eventually purchased should be based on the highest minimum requirements of ALL software that will be utilized.

NOTE (2): Hardware technology is constantly changing. The technical specifications recommended in this report represent current computer hardware industry standards as of the date of publication. This report will be revised periodically to provide updated technical details. For the most current hardware specifications at any time, you should consult hardware manufacturers' websites.

Computer hardware can have varying combinations. They can be standalone computers or they can be connected by a network, which may or may not be connected to a local server. Below is a brief list of components:

2.1 Workstation computers

A “work station” or a “workstation computer” is a computer that is dedicated to a specific task. It may or may not be connected to another workstation or network server.

The user's choice of a specific workstation will need to take many different factors into consideration. The most important factor will be the specific minimum hardware requirements of the software that will be run on it and the purpose for which it will be used. The requirements will be widely different for a workstation that is located in the user's front desk area (intended primarily for office management applications) and for one in the operatory used for digital radiographs, patient education videos and dental charting applications. Today, a work station can be a PC, laptop, tablet computer or a mobile device.

Some recommendations and guidelines that can be used for the user's selection are:

- A Central processing unit (CPU) — the fastest that the user can reasonably afford is recommended, but chosen for the application that the user will be running. For instance, office management applications and e-mail do not require the fastest, latest generation CPU to function well.
- B Operating system- The user's choice of operating system will depend on answers to many questions, including:
 - 1. Which operating systems (OS) support the user's software?
 - 2. Does the user's hardware have requirements *not* supported by other operating systems?
 - 3. What level of support will the user need to obtain from a third-party for the user's system?
 - 4. Does the user require a higher level of security due to the data it contains, e.g., PHI (protected health information)?
 - 5. Does the user want to restrict access to parts of the system or files?
 - 6. How long will the software be supported?
 - 7. Is the OS compatible with ALL software and hardware (digital radiography, photography, clinical charting, etc)?
- C Random access memory (RAM) — The amount of RAM will be dictated both by the operating system minimum requirement and the programs that will be running simultaneously. Highly memory intensive graphic applications such as games, video applications, and/or programs that involve extensive mathematical computations (CAD (Computer Aided Design)), 3D applications or very large spreadsheets will run more efficiently and benefit from more memory. The minimum RAM requirement given by any company for its operating systems is usually just that, the minimum for function. It is recommended the user purchase double the minimum RAM specified by the software that will be running to obtain optimal performance.

- D Display adapter - Also referred to as a video card, the display adapter can be integrated on the motherboard (the main electronic board to which all other parts are attached) or be an add-on. Make sure that it meets or exceeds the user's individual requirement. Higher end graphics cards are preferred for video applications.
- E Sound card, speakers, and microphone — If the workstation is intended for patient education, staff training, voice activated applications, or internet phone/video services, an appropriate sound card will be required. Speaker and microphone can be substituted with a microphone headset.
- F Digital camera (these can be still or video) — Use of digital cameras can provide extensive support for documenting the course of treatment, assisting in patient education and/or online conferencing. There are multiple ways that these cameras may be attached to the user's computer.
- G Hard disk or drive — A computer may be able to have multiple drives installed at any given time for additional storage space. Purchase a drive(s) that will meet the storage requirements for chosen programs and data. Note that if all data is stored on a server, the workstation hard disk requirement will be less. Video, digital radiography and digital photography files increase the storage requirements significantly, thus, plan accordingly. If imaging is planned as part of the user's system, it is likely the workstation will be networked to a server (see additional recommendations below). However, if the user plans image storage on the workstation, it is recommended that the user ascertain the requirements of the imaging system – some digital radiographic files are larger than others – and purchase a drive of sufficient size to store at least three years' worth of images. (Note: the dentist's malpractice carrier and/or legal counsel should be consulted regarding recommendations for retention of records, including images as they pertain to the user's specific policy and/or local jurisdictions). Hard disk solutions also shall include a redundant array of independent disks (RAID). Such solutions will help to avoid data loss and will aid in expeditious data recovery. These solutions can vary from local to cloud based services.
- H Compact disk-read only (CD-ROM) — Any of the current CD-ROM drives from a brand name company are acceptable.
- I Writeable CD (CD-R) — This drive may be used to replace the standard CD-ROM and be used for writing CDs for data/program backup and other computer data, such as digital images, etc.
- J Re-writeable CD (CD-RW) — Similar to the CD-R drive, this drive can use special CD-RW disks multiple times, much in the same manner as the traditional floppy disk.
- K Digital versatile disk-read only memory (DVD-ROM) — This high capacity computer software and data storage media is a read-only format. Educational software, software programs, and video can be included on a single disk.
- L Digital versatile disk (DVD Media) — There are 3 main forms: DVD-RAM (can only be read in drives that are DVD-RAM compatible); DVD-R/DVD-RW (DVD "dash" (or DVD "minus" outside the US)); and DVD+R/DVD+RW (DVD "plus"). The last 2 can be written and rewritten.
- M Blu-ray- Any of the current Blu-ray player from a brand name company is acceptable; these are read only.
- N Backup system — Backup is essential. A local backup can be made via a fixed or removable drive. The media can be a CD, DVD, flash drive, solid state drive or an additional drive. A redundant form of backup that is off-site is highly recommended. The redundant back up can also be in form of a remote (off site) backup service or a cloud based service.
- O Network card – Ethernet (Ethernet is a family of frame-based computer networking technologies for local area networks) connections provide the safest and most reliable connections. Wireless cards can also be utilized, but they are generally slower and not as reliable and/or as easy to set up. The efficiency of the system will be dependent on the slowest component within it.

2.2 Server computer(s)

A server is a network computer that acts as the centralized data storage device for workstations connected to the network. A server can be dedicated – where it runs in the background, or act as an additional workstation – a so-called “peer” server.

The user's choice of a computer to act as a server will need to take several questions into consideration: the operating system to be run; the number of workstations on the network; the specific minimum hardware requirements of the dental practice management software chosen for the office; and all the other software programs that may run on it if used as a peer server. Digital radiography, EHR and other imaging can change the requirements considerably. The recommendations will be the similar to those described above under Workstation Computers with the following additional recommendations:

- A Hard disk—the server stores data inputted from all workstations. If digital radiography or other forms of imaging are planned for the user's system, it is recommended that the user purchase a drive(s) sized to accommodate the anticipated cumulative image storage needs of all workstations for at least a three year period of time in addition to the minimum recommended for the user's operating system and software programs combined.
- B Modem – If no other Internet access is available or if required by a specific software application broadband technologies like DSL (technologies that provides digital data transmission over the wires of a local telephone network), cable modems, etc. can be set up separately and be connected via an Ethernet cable or a USB cable.
- C Network card – Ethernet connections provide the safest and most reliable connections. Wireless cards can also be utilized, but they are generally slower and not as reliable and/or easy to set up. The efficiency of the system will be dependent on the slowest component within it.

2.3 Monitor

Choose the largest monitor that will fit in the space provided, especially if used for viewing images. A TFT (thin film transistor technology), an LCD (liquid crystal display) or a LED (light emitting diode) monitor is preferred, especially in clinical areas, since they are easier to use and to keep clean.

Refresh rate—In order to reduce eyestrain, especially in offices with fluorescent lighting, it is highly recommended that the display adapter/monitor be set to a refresh rate of 75Hz or higher.

Display resolution -- The software will determine the exact specifications. Digital imaging and or graphics may require higher resolutions in order to display images with full detail. For these technologies it is advisable to choose a monitor and display adapter which are capable of these higher resolutions to provide a clearer image.

Display size -- Larger displays will be able to provide a clearer image. This will also be determined by the distance of the user from the screen, the available space and the user's needs (clarity of the picture). As display resolution increases, text size decreases. To maintain readable text at normal viewing distances (18-24-in.), use the optimal resolution for that specific monitor.

- 2.4 **Display adapter** - Also referred to as a video card or a graphics card, this can be integrated on the motherboard or be an add-on. Make sure it meets or exceeds the user's individual requirement. If the intended use contains any video or 3D imaging, a dedicated graphics card of a high quality is recommended. Please check compatibility with software and hardware manufacturers.

Color depth -- Even a basic display adapter should be capable of the three standard color depths:

- A 8-bit (256 color, also known as palette color);
- B 16-bit (65,535 colors, also known as high color);
- C 24 or 32-bit color (16.7 million colors, also known as true color).

8-bit color is suitable for general office tasks only, such as word processing and basic patient management software; it is not recommended for any windows based programs. Digital radiographic software and computer-based intraoral imaging will generally need 16 or 24/32-bit color for proper display of color images.

NOTE: 24-bit and 32-bit color modes produce the same number of colors, 16.7 million. The extra 8-bits in 32-bit mode are used for transparency effects (typically used in 3D applications) and do not add additional colors. Higher resolutions are needed for TFT/LCD screens. In all cases check with the manufacturer of the user's specific imaging software (digital radiography and/or intraoral imaging) for recommendations on color depth.

2.5 Input devices

- A Keyboard: Standard 101/104 key keyboard or compact size keyboard.
- B Pointing device: 2 or 3 button mouse, trackball, pen tablet or other suitable pointing device. Most connect via a USB port, some still connect via a PS/2 connector. Flat surface keyboards and other wireless input devices are preferred for clinical (in-operatory) workstations to facilitate infection control.

2.6 Video capture cards

Video capture cards are used to take an analog video signal from a video source (such as an intraoral video camera) and digitize it so it can be displayed and/or stored on a computer. Although there are many video capture cards available, it is best to get recommendations from the camera's manufacturer for particular models which have been tested to be compatible with their specific camera model and software. This video capture card compatibility will determine the resolution of the image

2.7 Printers

Printers can be divided into two basic types depending on their intended uses and features: black and white or color printers. Black and white laser printers are primarily used for normal office printing tasks such as letters, billing statements, etc. Black and white laser printers are not generally suitable for printing images such a digital radiograph or video camera image. If the user's office requires printing of multi-part or NCR (carbonless) forms, then a dot matrix printer may also be required.

Color printers can be broken down into three common types; color inkjets, dye sublimation and color laser printers. Color inkjets (which may include solid-ink systems) are, by far, the most adaptable and may be used for printing digital radiographic images and digital video camera images.

Another common type of color printer is the dye sublimation printer. It is excellent at producing lifelike color images from digital video camera images and may be suitable for printing digital radiography images as well. Some dye sublimation printers are only capable of printing on smaller-than-letter size paper and card stock, such as 4-inch x 6-inch photographic type paper. The user should check to make sure the smaller paper size is supported by the software if this type of printer is to be purchased.

Color laser printers are now widely available and may be more cost effective if large volumes of color images are needed and speed is a concern. Color laser printers are the fastest color printers, followed by the ink jet systems. Dye sublimations printers generally produce the finest pictures, but are very slow, and the operating cost is high.

A general recommendation is to have both a black and white laser printer in the front office area and a color laser for printing digital radiography and other images. A dye sublimation printer could be added for printing digital video images, but is not recommended as the only type of color printer in an office due to its limited use and slow printing speed. Keep in mind that the cost of consumables such as ink and special paper can easily exceed the cost of the printer if many images need to be printed. For optimum print quality, it is important to use high quality paper specifically designed for the type of printing the user intends to do. A common mistake is using copy or laser paper with

inkjet printers. While such paper is fine for use in copiers and laser printers, inkjet printers require paper that is designed for inkjet use in order to produce high quality output. An inkjet printer is only as good as the paper utilized.

When selecting a printer, the most important issues to address are:

A Intended use of the printer:

1. Number of users supported – A printer intended to support several users simultaneously, or intended for extensive printing, should be a higher speed network printer with additional memory;
2. Multi-part forms – dot matrix;
3. Billing statements, reports, etc – black & white, or color laser;
4. Digital radiographs – ink jet, or high resolution laser;
5. Digital images (photographic) – color ink jet, color laser, or dye sublimation (higher memory requirement).

B Total cost of ownership:

1. Initial cost;
2. Cost of consumables;
3. Availability of supplies and support (including optional extended warranties, if purchased);
4. Ease of service;
5. Number of users supported.

C Physical footprint (space required for installation and access during use).

D A printed digital radiograph is **NOT** considered to be solely adequate to support a clinical diagnosis. (See *ADA Technical Report No. 1023 for Implementation Requirements for DICOM in Dentistry*.)²

2.8 Data redundancy and backup

Refer to *ADA Technical Report No. 1021 for Recommendations for Data Redundancy* for more detail on this subject.³

Backup refers to making copies of data so that these additional copies may be used to restore the original after a data loss event. This is a very important task and should not be taken lightly. Keep in mind the time, effort and cost that would be needed to manually re-enter all data if it is lost. More importantly, can the user even reconstruct all of the information? As with all aspects of medical records, the HIPAA privacy and security laws should always be considered and the data protected at all costs.

For simplicity, all data should be stored on a centralized computer or server. This computer should have the capability to store multiple copies of the user's critical data simultaneously on separate disks (redundant data), as well as a backup system that can be used unattended. The most common backup system is an automated backup system that allows the user to decide when the backup occurs as well as what needs to be backed up. Generally, the backup operation itself should occur after normal working hours, as data cannot be backed up if it is being used. Backups should be made nightly. A redundant remote backup to a secure off-site server is advised. There are many third parties offering this service.

The method of storage will depend on what the user will be backing up. There are many ways to do this, including, DVD/RW, tape backups, external drives, cartridges, solid state drives, USB flash drives, cloud back-up, etc. If the users have any type of digital images on these computer(s), they will need larger capacities.

Please keep in mind that almost all backup systems list their capacities assuming a 2:1 data compression when backing up data to the drive. If the data on the user's hard drive(s) is already highly compressed, i.e., there are many JPEG image files, it is likely that no further compression will occur and the actual backup capacity will be half of the stated capacity.

Hard disk solutions also shall include a redundant array of independent disks (RAID). Such solutions will help to avoid data loss and will aid in expeditious data recovery.

2.9 Uninterruptible power supplies

Computers with critical data stored on them should always be connected to an uninterruptible power supply (UPS). In the case of a power outage, a UPS will provide power to the computer for a short time, enabling it to be safely shut down. Abrupt power failures or brownouts can cause loss and/or corruption of data on computers that are not connected to a UPS.

Most importantly, servers must be connected to a UPS and should have power-monitoring software that will properly shut down the server if the power outage exceeds a certain time period. In case the power failure happens at night when the office is unoccupied, especially during a back-up, monitoring software will tell the server operating system to close all files and then properly shut down. This is vital to prevent data loss or corruption. Data loss or corruption may not clearly be evident and may not cause problems until long after the power failure. Batteries should be tested and replaced regularly or at manufacturers' recommendations.

2.10 Surge suppressors

Any computer that does not warrant the protection of a UPS, as well as peripherals such as monitors, printers and scanners, modems, etc., should be connected to a surge suppressor to protect against line voltage surges and damage from lightning strikes to the utility lines. Models whose quality and reputation are consistent with the value placed on the equipment and data being protected deserve serious consideration for acquisition.

2.11 Network hardware

Since network hardware speed has been increasing in the last few years, all new network installations should use at least Gigabit Ethernet, as discussed later in this document.

- A **Modem** – If no other Internet access is available or if required by a specific software application broadband technologies like DSL (technologies that provides digital data transmission over the wires of a local telephone network), cable modems can be set up separately and be connected via an Ethernet cable or a USB cable.
- B **Network card** – Ethernet connections provide the safest and most reliable connections. Wireless cards/networks can also be utilized, but they are generally slower and not as reliable and/or easy to set up. The efficiency of the system will be dependent on the slowest component within it.
 - 1. **Network interface cards** – Network interface cards (NICs or just network cards) are used to connect a computer to a network cable of some type. These cards either may be add-in cards or integrated on the mainboard (aka motherboard) inside the PC.
 - 2. **Network cabling** – As with hubs and network cards, network cabling can affect the speed. Network cabling is rated as Category 5 for 100 Mb/s operation or Category 6 for Gigabit Ethernet. All new wiring should be at least Category 5. Shielded cabling is recommended over unshielded for dental offices, since this will protect the data from interference. Fiber-optic networks are much faster and much costlier than the Ethernet cabling mentioned above.
 - 3. **Network hubs and Network switches** – A network hub or switch is a central connection point for all computers on the user's network. It is commonly located near the server, but may be located anywhere in the office. It can be wired or wireless. Like the rest of the network equipment, the hubs should also be 1000Base-TX or higher.

A network hub, or repeater, is a fairly unsophisticated network device that distributes all the data it receives to all the network devices connected to it.

A network switch can be considered a smart hub. It will actively look at the traffic it receives and based on the destination address, it will direct that traffic only to the port of the connected device needed.

Hubs do not manage any of the traffic that comes through them. Any packet entering a port is broadcast out or "repeated" on every other port, except for the port of entry. Since every packet is repeated on every other port, packet collisions result, which slow down the network. There are specialized applications where a hub can be useful, such as copying traffic to multiple network sensors. High end switches have a feature which does the same thing called port mirroring. There is no longer any significant price difference between a hub and a low-end switch.

C Universal serial bus (USB)

A standardized connector for interfacing various devices to a host computer, USB was designed to allow many peripherals to be connected using a single standardized interface socket and to improve plug-and-play capabilities. USB is intended to replace many legacy varieties of serial and parallel ports. USB can connect computer peripherals such as mouse, keyboards, PDAs (Personal Digital Assistant – a hand held device), gamepads and joysticks, scanners, digital cameras, printers, personal media players and flash drives. For many of those devices USB has become the standard connection method. USB2 ports transfer data 40 times faster than USB1 ports, and USB3, 400 times faster. The user should select a computer with a sufficient number of USB ports to accommodate the varied peripherals they plan to connect to it. Currently most USBs are the 3.0 standard. All devices should be at least 2.0.

D Remote access

A computer can be set up to be accessed remotely and also be able to take control of any computer in a network when it is set up appropriately. This can be done through an intranet or the internet

E Wireless networking

Wireless networks have continued to develop and their uses have grown significantly. These include Wi-Fi and cellular networks and Bluetooth protocols. Another important use for satellite and cellular wireless networks is as an inexpensive and rapid way to connect to the Internet, especially in rural areas where wired infrastructure may not be present. Wireless networks may require extra configuration to resolve connection issues, but are very convenient and less expensive to set up than wired networks, especially if cable installation is required. Older wireless networks typically are slower and less reliable than those connected directly through a network cable, but newer technologies have improved this technology. Most devices today have built in wireless connectivity. Newer devices may no longer ship with wired connections.

A wireless network does require additional security to prevent unwanted access. Protocols such as Wired Equivalent Privacy (WEP), the newer Wi-Fi Protected Access (WPA), or the even newer and more secure Wi-Fi Protected Access II (WPA2) should be implemented to enhance network security and control access to the network. In addition, no public access should be given to the wireless network. Should the office wish to offer Wi-Fi access to non-practice mobile devices, this should be done on a separate, isolated guest network. Many routers offer wireless "guest" dual-network capability.

To prevent security breaches, use of firewalls should be mandatory. Updates to both the router and computer operating systems should be made regularly to fix security issues. A practice may also have dental equipment that can interfere with or restrict wireless communication.

F Firewall

A firewall secures a network by inspecting traffic passing through it and denies or permits passage according to a set of rules, based on preset "trust" levels. A firewall's function within a network is to prevent network intrusion, but without proper configuration, a firewall can often become ineffective. Firewalls can exist on servers and on individual workstations in the form of software, or at the perimeter of a network (usually in a router) as a type of hardware called "firmware" (firmware is the fixed, usually rather small, programs and/or data structures that internally control various electronic devices). Thus, the firewall can be host-based or network based.