American Dental Association
Revised Technical Report No. 1055

Computer Hardware and Software Guidelines for Dental Offices

ADA American Dental Association®

2016

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.

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.