

American Dental Association
Technical Report No. 1031

Internet Security Issues for Dental Information Systems



American Dental Association 2004



Documents

Document Sharing Hub



Documents

Copyright © 2004 American Dental Association. All rights reserved. Any form of reproduction is strictly prohibited without prior written permission. Document Sharing Hub

AMERICAN DENTAL ASSOCIATION TECHNICAL REPORT NO. 1031 FOR INTERNET SECURITY ISSUES FOR DENTAL INFORMATION SYSTEMS

The Council on Dental Practice of the American Dental Association has approved American Dental Association Technical Report No. 1031 for Internet Security Issues for Dental Information Systems. Working Groups of the ADA Standards Committee on Dental Informatics (SCDI) formulate this and other technical reports and specifications 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. Approval of ADA Technical Report No. 1031 was confirmed by the ADA SCDI on April 12, 2004.

The ADA SCDI thanks Norman Schreiber, HIPAASeminar.com, Phoenix, MD, as chairman of Working Group 10.3 for Dental Information Systems Security and Safeguards for leading the development effort.

AMERICAN DENTAL ASSOCIATION TECHNICAL REPORT NO. 1031 FOR INTERNET SECURITY ISSUES FOR DENTAL INFORMATION SYSTEMS

FOREWORD

(This foreword does not form a part of Proposed American Dental Association Draft Technical Report No. 1031 for Electronic/Digital Signatures Uses in Dentistry).

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:

“To promote patient care and oral health through the application of information technology to dentistry’s clinical and administrative operations; to develop standards, specifications, technical reports, and guidelines for: components of a computerized dental clinical workstation; electronic technologies used in dental practice; and interoperability standards for different software and hardware products which provide a seamless information exchange throughout all facets of healthcare.”

This technical report was prepared by SCDI Working Group 10.3 for Dental Information Systems Security and Safeguards. The SCDI Working Group 10.3 chairman is Norman Schreiber. SCDI Working Group 10.3 prepared this report at the request of SCDI Subcommittee 10 for Dental Informatics Architecture and Devices (Scott Trapp, Chairman).

AMERICAN DENTAL ASSOCIATION DRAFT TECHNICAL REPORT NO. 1031 FOR INTERNET SECURITY ISSUES FOR DENTAL INFORMATION SYSTEMS

SCOPE

The Scope of this Technical Report is to create security awareness and education for the dental practitioner associated with a connection to the Internet. The Internet has proven to be an effective means of communication, yet its vulnerability to interception raises issues of privacy, authentication and integrity of the communicated message. Therefore, data security is of utmost importance to users of dental information systems

Because of the personal and private nature of health record, the dental practitioner needs to understand the security issues associated with “data at rest” and “data in transit.” This paper is intended to explain security concepts and the risks associated with the maintenance of data in storage and transit, and over an Internet connection.

INTRODUCTION

Whether health care businesses will make use of the Internet is no longer debatable. Internet use among all businesses is growing at accelerating rates. Even small businesses have jumped on the Internet bandwagon, with use climbing from 35 percent in 1996 to a projected 76 percent by 2003.¹

The Internet is a global communications system that allows users to obtain information at an unprecedented scale and scope. Its effects on healthcare systems are only beginning to be realized. E-mail traffic still makes up the largest portion of Internet use by small business, but electronic commerce and transactional applications, such as electronic claims, are on the increase as well. The most successful emerging business model for the Internet is as an additional tool for business-to-business transactions.

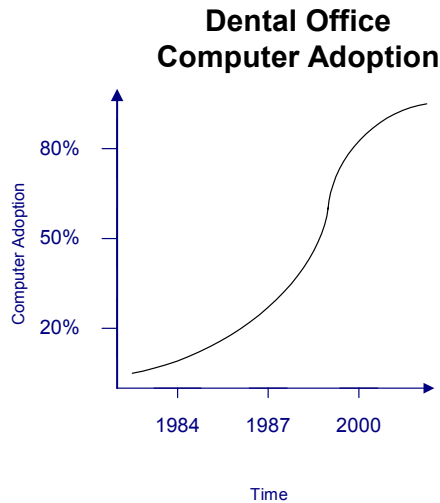
An estimated 96,000 dentists (66.8 percent) had a computer in their office in 1997.² The percentage of dentists who have computers at work increased from 11.0 percent in 1984 to 79.5 percent in 1997. Modem availability has increased from 61.7 percent in 1995 to 69.1 percent in 1997.³ The percentage of dentists who have computers in their practice has increased steadily since 1984. The most recent rise being 5.6 percent from 1997 – 2000.⁴

In dentistry, dental team members routinely communicate with external entities such as other dentists, healthcare providers, patients, payers and dental suppliers. Patient records, textbooks, journals, product information and colleagues serve as information resources. In many instances, information exchanged to effect a transaction never takes paper form. Computer-based information also can be utilized differently than its paper counterpart. For example, computers can “read” digital information and transform the information or take programmable actions based on the information. Information stored as bits rather than as atoms of ink and paper can travel near the speed of light, and may be duplicated without limit or significant cost. The Internet adds a new and powerful resource to the dental office by improving efficiency and accuracy of communication, and by enabling access to current and relevant information for supporting patient care.⁵

A 1998 study found that dental professionals obtained diagnostic and product information, discussed clinical cases, and communicated with patients on the Internet.⁶ Each time a patient

sees a health care provider, is admitted to a hospital, goes to a pharmacist or sends a claim to a health plan, a record is made of that event and a transaction occurs adding data to his/her confidential health information. For many years, our family health care providers, hospitals, and pharmacies maintained the confidentiality of those records, keeping them protected and sealed away in file cabinets, refusing to reveal them to anyone else.⁷

There were strict protocols for requesting and transmitting this information and postal service, courier, or other secure methods were utilized.



With the rise of Internet usage in communication and transmission for patient treatment, referral, and payment, this private information is available to anonymous and clever companies and people whose use of this information is questionable if not harmful. Inexpensive and accessible open networks are supplanting the formerly exclusive, expensive, slow, and limited-function delivery and communication channels. Since open networks are inherently less secure than the closed networks,

electronic commerce increasingly depends upon securing and authenticating the information itself, rather than relying only upon the security of the channel (phone line or browser) and validity of the sender.

Consider the number of viruses that have been passed thru Email by imposters and the damage they do. Imagine what could happen to providers and healthcare systems by fraudulent individuals submitting information to payers, health plans, specialists, suppliers and other providers. Identity thieves search for information in the physical world, collecting names, social security numbers, addresses, credit card numbers and other bits of data they can use to bilk their victims. Merchants and credit card companies use *non-repudiation* measures, such as the use of a personal identification number (PIN) mother's maiden name, or other means, to aid in the identification of frauds and approve legitimate transactions.⁸

There are *authentication*, *privacy* and *integrity* issues associated with this new open format of communication. As technology has proliferated and databases of all types grow in number and depth, more attention finally is being focused on their privacy and security. *Privacy* refers to the right of individuals to control access to personal information. *Security* refers to the tools put in place to enforce privacy and protect information systems. In the area of health information, both privacy and security are significant concerns. While this problem is not new, or unique to electronic systems, the potential for abuse and the visibility of the issue is raised as records move from paper to electronic forms of collection, storage, and use.

Health care providers and payers currently are increasing use of electronic claims submission using Electronic Data Interchange (EDI); however, the Internet is quickly emerging as an alternate method of choice. Security, authentication, integrity and privacy of electronic transactions, along with further development of the electronic health record, use of DICOM radiographic image files and Email for communication with other health care providers, organizations, suppliers, and patients, will test our skills to secure the internet portal to which we connect.

While excellent progress has been achieved in Internet communications, very little has been done to inform users of the vulnerability of data at rest or in transit. Users also lack information about reducing the risk of threats to information such as unauthorized modification, questionable authentication, information disclosure and destruction—whether deliberate or accidental.⁹ To make significant progress, dentists' concerns will have to be addressed. The need for private and secure communication has become obvious in the cyber world, which is populated increasingly by eavesdroppers, cell phone number thieves, credit card imposters, and fraudulent e-mailers.

This paper will discuss the security issues associated with dental information systems, but will not provide the dentist information on electronic/digital signatures. These issues are discussed in ADA Technical Report No. 1016 --Electronic/Digital Signature Uses in Dentistry.

DATA SECURITY AND THE LAW

The Federal government and the public have growing concerns regarding the security of computer based information systems. The Internet does not have national boundaries, immigration officers, or customs services like ports of entry in the real world; it is a seamless global network. Because businesses are increasingly dependent on computer networks, potential business losses stemming from a security breach are possible. Even if a hacker fails to access confidential data or read a user's e-mail, he/she may have inserted a virus, and the system owner would have to assume the worst. The owner would have to take an entire network segment and its trusted hosts off-line in order to investigate and repair the damage.¹⁰

As a response to growing public and private concern, the House Science Committee approved H.R.2413, The Computer Security Enhancement Act, in July of 2000.¹¹ The bill reaffirms the National Institute of Standards and Technology's (NIST) responsibilities to work with voluntary private sector standards organizations in the development of civilian agency data security standards. The bill prioritizes developing security guidelines and protecting sensitive federal information.

As part of the HIPAA legislation, the Health Care Financing Administration (HCFA) and the Department of Health and Human Services (HHS) published a Notice of Proposed Rule Making (NPRM) for security. This NPRM addressed HIPAA's (Health Insurance Portability and Accountability Act) proposed requirement for a national security standard for data in transit and at rest. It includes administration of standalone systems as well as networked systems with or without modem connection and technical security services and mechanisms.

Within the aforementioned law, security "... encompasses all of the safeguards in an information system, including hardware, software, personnel policies, information practice policies, disaster

preparedness, and the oversight of all these areas. Information security is needed to protect both the system and the information it contains.”¹²

This definition was written in generalized terms to allow for some economy of scale; defining the concepts of adequate data security was more important than describing how to implement it. Larger entities like clearing houses and insurance companies have different security needs than small, private practices; as long as the conditions of proposed rules or its successor regulations are met, a practice may be said to be in compliance.

THE INTERNET: DEFINITION AND HISTORY

The Internet began as ARPANET, the Advanced Research Projects Agency Network, in 1969. Since that time it has become the world’s largest computer network. The Internet is currently a thriving forum for information, commerce, free speech and self-expression. Although the Internet has become a rich source of information, the quality and authenticity of this information is questionable due to the anonymity of its millions of users. Hackers, frauds, and other electronic felons can use this anonymity to exploit users, launch attacks against their systems and steal identities.

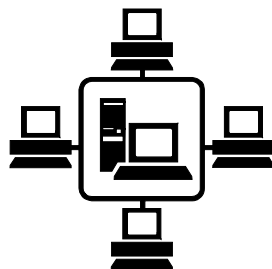
One of the original goals of the ARPANET project was to create a network that would continue to function even if major sections of the network failed or were attacked. ARPANET was designed to reroute network traffic automatically around problems in connecting systems, passing along the necessary information to keep the network functioning. From the beginning, ARPANET was designed to be robust against denial-of-service attacks. ARPANET protocols (the rules of syntax that enable computers to communicate on a network) were originally designed for openness and flexibility, not for security. ARPA researchers needed to share information easily, so everyone needed to be an unrestricted “insider” on the network.¹³

As more locations with computers (known as sites in Internet parlance) joined ARPANET, the usefulness of the network grew. ARPANET consisted primarily of university and government computers, and the applications supported on this network were simple: electronic mail (Email), electronic news groups, and remote connections to other computers.

In 1988, ARPANET had its first automated network security incident, usually referred to as “the Morris worm.”¹⁴ This “self-replicating automated network attack tool” caused a geometric explosion of copies to be started at computers all around ARPANET. The worm used so many system resources that the attacked computers could no longer function. As a result, 10% of the U.S. computers connected to ARPANET effectively stopped at about the same time.

The Morris worm prompted the Defense Advanced Research Projects Agency (DARPA, the new name for ARPA) to fund a computer emergency response team, now the CERT Coordination Center, to give experts a central point for coordinating responses to network emergencies. Other teams quickly sprang up to address security incidents in specific organizations or geographic regions.

In 1989, ARPANET officially became known as the Internet and evolved from a government research project to an operational network; by then it had grown to more than 100,000 computers.



Security problems continued, with both aggressive and defensive technologies becoming more sophisticated. In 1994, intruder tools were created to “sniff” packets from the network easily, resulting in the widespread disclosure of user names and password information. In 1995, the method that Internet computers used to name and authenticate each other was exploited by hackers who developed a new set of attack tools. This led to widespread

Internet attacks on computers with many trust relationships where the user relied on authentication, integrity and confidentiality of stored or shared information. Today, the use of the World Wide Web and Web-related programming languages creates new opportunities for network attacks.¹⁵

Many practices today have one or more computers and these can be interconnected. A *network* is a series of computers that have a connection limit determined by the distance data can be transferred over a connection wire to their network cards.

LANs are local networks because connected computers must be within 600 feet of each other. These computers contain network cards and are connected together with specialized cable. Every device on the network is assigned a unique address (a special set of numbers and letters). Information is sent to networked computer (s) or device (s) (a peripheral), by using a data packet. This data packet consists of information pieces-- a destination address and the sender address. Thus, the Internet is a loose association of thousands of networks and millions of computers across the world that all work together to share information. If we use the metaphor “information superhighway” and continue the transportation analogy, we can further develop the concept. We will think of the Internet as a mass transit system that crosses the United States. A series of smaller subway systems intersects the mass transit system at certain points along the way. Connecting to the smaller subway systems are other means of transportation such as, commuter rails, light rail, bus lines and ferry boats that spread out and crisscross the metropolitan areas.

These are the Internet backbone companies of yesterday, which have changed through merger and acquisitions. In addition to analog (dial-up) telephone, we now have cable and satellite companies as well as digital telephone service(DSL or Digital Subscriber Line).

To use the Internet a computer must use a modem (a device that encodes and decodes (modulation and demodulation) information. A modem is a telephone for the computer, it enables the computer to call and connect to another computer using telephone, satellite or cable lines sending data packets consisting of information pieces. One could imagine additional information pieces attached to the packet, among them a destination and sender address. Imagine that envelope and data packet moving along throughout the entire world looking for that destination address at the speed of light.

Computers using cable, satellite and DSL are always connected presenting a full-time security flaw, while dial -up is connected only at the time of use. *They are all vulnerable to attack.*¹⁶

BROADBAND CONNECTIVITY

To get online, one needs to connect your PC to a broadband modem, which in turn connects to the

broadband service. Typically, you will need an Ethernet adapter to connect your PC to the modem. This can be an internal card or an external USB-to-Ethernet adapter. (While such adapters run at about a tenth the speed of an internal card, they are still fast enough to keep up with the throughput of a broadband connection). Alternatively, your modem may support direct USB connections, in which case one just runs a USB cable from the device to your PC. With DSL or satellite, you will probably need to use with the modem your provider offers; with cable service, many people rent cable modems from their providers, but you may be able to purchase your own DOCSIS-compliant (Data Over Cable Service Interface Specification) modem.

CABLE

Cable enters your house via the same line as cable television. If cable TV is not available, you are unable to get cable broadband. However, getting cable TV does not mean one can get cable broadband; not all cable providers offer it in all areas. If cable broadband is available, the cable company typically is your single point of contact for all provisioning (preparing the line), installation, and service. Since fiber-optic TV cables were created for large data streams, the service is reliable and troubleshooting relatively simple. On the downside, cable users are on local nodes that share bandwidth; more people joining your node means less throughput available to you.

DSL

DSL runs over plain old telephone service (POTS) lines. Internet traffic travels on the same line as voice signals; filters on your telephone jack separate the two. On the positive side, everyone has phone lines. On the negative side, the P and O in POTS are important. Most telephone lines were not run with data traffic in mind. Often, they are not DSL-ready. Also, your computers need to be within a certain distance of the central office (a telephone switch) or you can not get service. The distance allowed varies, but generally it's 15,000 to 18,000 feet—as the wire runs, not as the crow flies. Insist on knowing your distance and the company's maximum service distance. If your case is borderline, pursue other options or wait until a Central Office is closer. When DSL works, your internet connection will be functioning, but you have no reliable way of knowing the condition of your phone lines until you have tried them.

SATELLITE

Satellite's advantage is that theoretically, all PC owners with electricity and a clear view of the southern sky can receive the satellite signal. Basically, satellite Internet traffic travels from a ground-based network operations center (NOC) to a satellite and from there to one's computer. Customers in rural areas who may wait years for cable service and might never obtain DSL can benefit from satellite. Others will want to avoid satellite's disadvantages: relatively low throughput, service that may be affected by bad weather, and high setup and monthly costs.

NETWORKING

If just one broadband connection for multiple PCs is available, one should network them! With a network one can share not only connectivity but also printers and files; one can view and share streaming media. First, determine your network needs, and then choose a technology based on those needs, and your office's layout. Second, buy and install hardware. Third, configure everything to work securely .

USE OF A ROUTER

No matter how data is moved between devices, one needs a way to direct the traffic. The least costly option is part of all versions of Windows from Windows 98 SE on: Internet Connection Sharing, or ICS. It is the least costly method, but not the best solution. Instead, consider an inexpensive broadband router. Computers in an office network connect to the router, which in turn connects to a modem. Most routers include firewalls, which one needs anyway, as you will see in the "Safe Connections" section.

ETHERNET

100-Mbps Ethernet is the fastest office networking technology. If all of your PCs are in a single room, and they are not portable, a small, 100-Mbps switched Ethernet network is the least costly solution. Ethernet networks are reliable and easily maintained, and many devices ship with built-in network ports. On the other hand, running cables and installing jacks throughout the office can be expensive.

If the computers do not have built-in Ethernet ports, one will need to put a network interface card (NIC) in each machine or attach a USB Ethernet adapter. USB adapters are easier to install, and they should provide adequate speed for most users. Connect the cable or DSL modem to the LAN or external port on your broadband router and connect the other computers to the internal switched ports.

WIRELESS 802.11b

If one wants to carry a laptop around the office, 802.11b wireless access is the preferred way to go. Ranges vary by product—and with the level of interference from large metal objects, ceilings, walls, microwaves, and 2.4-GHz phones. As with Ethernet, one needs to understand the office layout.

The first decision to make is whether to install your wireless network in "point-to-point mode or infrastructure mode." If there are only two PCs to connect and one is willing to rely on the dreaded ICS, you can use "point-to-point" access. Otherwise, use infrastructure mode, which requires an access point (AP)—like a hub for your wireless network. It is possible to buy a broadband router with a built-in AP, which is the best bet in terms of price and ease of installation and management.

Keep in mind that it is difficult to confine the wireless signal to the inside of your office. During initial configuration one should also change the default management password. Also, remember to enable Wireless Encryption Protocol (WEP)—or the newer standard, if available—and write down the key. WEP isn't perfect, but it discourages casual hackers.

Finally, use any other means to lock down the wireless LAN that your AP offers, such as restricting the MAC addresses (the unique IDs of all network cards) that can access the WLAN, or limiting the number of leases handed out to the number of computers you own. Solutions vary by AP; check your documentation.

IS BROADBAND SAFE?

As discussed earlier, on the Internet nobody knows your name, but every site you visit knows your IP address. This IP address identifies computer, and it is the starting point for any attack. Dial-up

(analog) service is a moving target: one needs to get a new IP address for each connection. Broadband connections typically have static, always-on IP addresses, so if a hacker manages to break in, he is less likely to lose the connection and can come back later. If the compromised system is connected to a network that uses TCP/IP rather than the NetBEUI or IPX protocol, the whole network may be exposed.

Data is not the only items hackers want, hackers still can use the machine to launch attacks on bigger targets, particularly in DDoS (distributed denial of service) attacks.

HOW SAFE IS CABLE MODEM ACCESS?

Some older cable modems have a special kind of vulnerability that makes a system and others nearby effectively form a local area network. If a system is configured incorrectly, its drives can show up in your neighbor's computer's Network Neighborhood. To solve this problem, some Internet service providers(ISP) encrypt all cable modem traffic, while others use a strictly router-based connection with no LAN-type connection to nearby users. It is suggested that users find out what security measures their ISP employs. One should also install a hardware or software firewall. If file and printer sharing are not needed, turn it off.

HOW SAFE IS DSL ACCESS?

Unlike cable, DSL offers point-to-point connections with the phone company's switch. Each DSL customer has a unique connection called a Private Virtual Circuit that secures his/her connection with the ISP. Occasionally, however, specific DSL modems contain security flaws. For example, problems with some Alcatel modems were reported in 2001. It is important to perform a Web search on the make and model of your DSL modem to see whether it has any known problems.

HOW SAFE IS SATELLITE ACCESS?

A geo-stationary satellite (about 22,300 miles high) is a stable target, but the quarter-second round trip for each packet causes latency problems. In low earth orbit (about 1,000 miles up) the latency problem is reduced, but this technique requires a network of satellites and a mechanism to switch between them. Some systems try to defeat the latency problem via TCP spoofing, which can conflict with VPN (virtual private network) solutions. Others actually incorporate a VPN, which precludes using one's own customized VPN. Some satellite ISPs encrypt all traffic. It pays to check with the ISP to determine its security measures. Eavesdropping should not be an issue. The signal usually is shared using cell phone security techniques, CDMA, TDMA, or FDMA (Code, Time, or Frequency Division Multiple Access); it does not reveal a simple coherent data stream.

SECURITY FOR DENTAL INFORMATION SYSTEMS

Today, many employees in a dental practice commonly look at the contents of patient healthcare records and connect to the Internet to "surf" or use e-mail. With the ability of browsers to automatically save passwords (unless turned off), share passwords, etc., the security risk is elevated to dangerous levels. Unauthorized and unauthenticated individuals from within or without might gain access to business and patient information and possibly release or alter that information.¹⁷

Computer security is the combination of process, procedures, and tools that assure data entered into a computer today will be retrievable at a later time, and only by those authorized to do so. This