ADA Technical Report No. 1019
Approval date: January 28, 2003

American Dental Association
Technical Report No. 1019

Technical Security Services

ADA American Dental Association 2003

AMERICAN NATIONAL STANDARD/AMERICAN DENTAL ASSOCIATION TECHNICAL REPORT NO. 1019 FOR TECHNICAL SECURITY SERVICES

The Council on Dental Practice of the American Dental Association has approved American Dental Association Technical Report No. 1019 for Technical Security Services. 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. 1019 was confirmed by the ADA SCDI on January 28, 2003.

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 NATIONAL STANDARD/AMERICAN DENTAL ASSOCIATION TECHNICAL REPORT NO. 1019 FOR TECHNICAL SECURITY SERVICES

FOREWORD

(This foreword does not form a part of American Dental Association Technical Report No. 1019 for Technical Security Services.)

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 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 Accredited Standards Committee MD156 (ASC MD156) evolved into the ADA Standards Committee on Dental Informatics (SCDI). The SCDI 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 NATIONAL STANDARD/AMERICAN DENTAL ASSOCIATION TECHNICAL REPORT NO. 1019 FOR TECHNICAL SECURITY SERVICES

CONTENTS

Summary……4
Introduction……6
Purpose……7
Scope……7
Background……7
Technical Security Services……11
Glossary……38
References……44

AMERICAN NATIONAL STANDARD/AMERICAN DENTAL ASSOCIATION TECHNICAL REPORT NO. 1019 FOR TECHNICAL SECURITY SERVICES

SUMMARY

Information security is not just about protection from hackers and viruses. In principal, it is about applying best practice methods to ensure that information systems are developed, maintained and operated in an orderly, controlled and secure manner for the economic benefit of the dental provider. It is also about obtaining an independent assessment of technical issues, which the provider may be able to assess himself.

Furthermore, because of real security risks to society, the provider is no longer the sole decider of what to secure and how to secure it. Today there is an increased risk of inadvertent or deliberate disclosure of Individually Identifiable Health Information in heath care information systems. Security standards are increasingly being dictated in regulation and legislation, imposing external compliance responsibility on health care. Securing health care information in a reasonable and scaleable manner can be achieved by applying policies and procedures designed to cover four major areas of information management. These areas are Administrative Procedures, Physical Safeguards, Technical Security Services and Technical Security Mechanisms. Use of an Electronic Signature is suggested to insure that authentication and non-repudiation requirements of Security are met in a standardized manner.

Congress mandated security and privacy rules as part of the HIPAA legislation. This occurred because storing and transmitting protected health information in an electronic format exposes it to additional risks that do not exist, or are lessened, when health information is in paper form. Securing patients' protected health information also protects their privacy and enhances the dentist's reputation for professionalism and trustworthiness.

The scope of this paper is to focus on those requirements for meeting the challenge of maintaining privacy and security of Individually Identifiable Health Information using Technical Security Services. These processes are put in place to protect information and to control and monitor individual access to information.

Many security and privacy requirements are clear and specific. The major requirements a dental office can meet are:

A Document security and privacy policies and procedures, and actions taken to ensure that policies and procedures are enforced.

B Assign responsibility for security to a designated individual.

C Develop a Security Gap Analysis and determine your risk.

D Assess risks and determine major threats to security and privacy of protected health information.

E Establish a program of Best Practices that are scaleable and reasonable to resolve risk issues.

F Adopt a privacy policy and publicize the policy by providing notice to all patients. Privacy policies should have specific provisions for gaining consent and/or authorization to use protected health information, restricting use and disclosure of protected health information, and receiving and resolving patient complaints.

G Set up a security management program, which addresses physical security, personnel security, technical security controls, and security incident response.

H Train staff (and business associates who work on the covered entity's premises) to follow proper security and privacy policies and procedures the office has developed. .

I Appoint a privacy officer and a point of contact for receiving privacy complaints.

J Change contracts and business partner agreements to ensure that partners handle protected health information properly.

K Certify the effectiveness of the Dental practices' security controls.

AMERICAN NATIONAL STANDARD/AMERICAN DENTAL ASSOCIATION TECHNICAL REPORT NO. 1019 FOR TECHNICAL SECURITY SERVICES

INTRODUCTION

HHS consulted with the American Dental Association throughout the process of developing and promulgating the first national standards for administrative reforms mandated by HIPAA ,and continues to consult with the association on security and other reforms being developed.

The first two national standards that have become law cover:

A Electronic reporting of dental and other healthcare procedures (issued August 2000), conformance with the standard by the dentist by October 16, 2002 unless you have requested a one time extension under HR 3323; [i]

B Privacy of individually identifiable health information (issued Dec 28, 2000), conformance with the standard by the dentist by April 14, 2003[ii]

Dentists are participating in shaping a new era of patient privacy. It's a new world of national standards converging at the nexus of Association policy, legislative mandate and regulatory framework.

Included in the new privacy rules, a typical dental practice will need to:

A Designate an office privacy official, who may have other duties as well

B Provide "plain language" notices to describing office policy practices

C Develop and document policies and procedures to secure Protected Health Information.

D Provide privacy training to employees

E Establish privacy agreements with " business associates"

F Obtain patient consent for disclosure of protected health information except for treatment by other providers and specified public policy.[iii]

The Privacy standard applies to information conveyed with electronic transactions but not limited to electronic transactions. [iv]The new rules are more sweeping than those proposed, covering not just electronic communication, but oral and written communication of individually identifiable health information held by dentists and other custodians of patient records, including their business associates, health plans and clearinghouses.

Development and implementation of Technical Security Services are necessary to insure requirements of privacy and security are met. All providers should have documented policies for processing health information. It is recommended that policies should cover both electronic health information and paper records. Many States already have their own Privacy laws that govern Healthcare Professionals and *security* needs to be in place so they are not violated.

PURPOSE

These Technical Security Service Guidelines provide a tool for developing policies, procedures, and best practices to assist the dentist in establishing security and privacy. These guidelines make recommendations for security and privacy implementation and maintenance within dental offices.

SCOPE

The intent of the paper is to provide guidance in the development of security and privacy policies and procedures that support all activities of complex dental environment. It is hoped that the results of this paper will assist the dentist in developing more efficient and inclusive ways of implementing health care security and privacy arrangements.

These guidelines recommend health information security and privacy mechanisms and strategies. Recommended strategies are intended to facilitate culture change by building upon existing best practice. They are based upon common understanding of practice processes. This effort also identifies implementation barriers that should be overcome, in addition to benefits or incentives that may be leveraged to deploy adequate resources within the individual practice.

This document does not provide legal advice, and covered entities should work with their legal staff to address appropriate requirements. This document may serve as a tool to expedite an understanding of necessary legal actions needed to address requirements, as well as federal and state legislation, as HIPAA has an impact on many aspects of dentistry.

On December 20, 2000, the Department of Health and Human Services Privacy Regulations were released. At the onset of this activity, it was impossible to determine when the draft privacy regulation would be made final, and how the final regulation might differ from the draft. The final privacy regulation was issued, but opened for comment again. The Bush Administration and HHS designated that the standard for Privacy would be implemented by April 14, 2003 for large organizations and April 14, 2004 for small organizations. At this date certain policy requirements are subject to possible change as well as their interpretation

BACKGROUND

Many dentists believe that health care information electronically collected, maintained, use, or transmitted is *already* kept confidential, private, and secure. Numerous states to date have passed laws providing for this. Security of health information is especially important when health information can be directly linked to an individual. Privacy can be considered the “what” of information and security the “how” to accomplish the requirements of privacy.[v] On February 13, 2001, Congress officially received notice of the final HIPAA privacy rule.

With passage of HR3323, the Administrative Simplification Compliance Act, a one-year extension of the date for complying with HIPAA standard transactions and code set requirements was provided. This requires submission of a plan detailing specific items. It is expected that most small dental provider practices will not have to worry about the technical specifications of transactions and code sets. This expectation is based upon speculation that practices will rely heavily on clearinghouses and their patient accounting or practice management system vendors for assistance in complying with HIPAA transaction standards (as well as many of technical components of the security and privacy standards). The standardized transactions must be used