

American Dental Association
Technical Report No. 1017

Administrative Procedures And Their Application to Dentistry



**AMERICAN DENTAL ASSOCIATION TECHNICAL REPORT NO. 1017 FOR ADMINISTRATIVE
PROCEDURES AND THEIR APPLICATION IN DENTISTRY**

The Council on Dental Practice of the American Dental Association has approved American Dental Association Technical Report No. 1017 for Administrative Procedures and their Application in Dentistry. 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. 1017 was confirmed by the ADA SCDI on September 17, 2002.

The ADA SCDI thanks Norman Schreiber, YourNameDDS.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. 1017 FOR ADMINISTRATIVE PROCEDURES AND THEIR APPLICATION IN DENTISTRY

FOREWORD

(This foreword does not form a part of the Dental Association Technical Report No. 1017 for Administrative Procedures and their Application 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 TECHNICAL REPORT NO. 1017 FOR ADMINISTRATIVE PROCEDURES AND THEIR APPLICATION IN DENTISTRY

SUMMARY

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 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.

This technical report will provide the dentist information on Administrative Procedures for Security and how they apply to dentistry to provide for policies, procedures and practices dealing with the behavioral side of the security and privacy standards.

Many security and privacy requirements are clear and specific. The major requirements a dental office must comply with are:

- A Document its security and privacy policies and procedures, and actions taken to ensure that policies and procedures are enforced;
- B Assign responsibility for security to a person;
- C Develop a Gap Analysis for Best Practices and determine your risk;
- D Assess risks and determine the major threats to the security and privacy of protected health information;
- E Adopt a privacy policy and publicize the policy by providing notice to all patients. Privacy policies must have specific provisions for gaining consent and authorization to use protected health information, restricting use and disclosure of protected health information, and receiving and resolving patient complaints;
- F Set up a security management program that addresses physical security, personnel security, technical security controls, and security incident response;
- G 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;
- H Appoint a privacy officer and a point of contact for receiving privacy complaints;
- I Change contracts and business partner agreements to ensure that partners handle protected health information properly;
- J Certify the effectiveness of the dental practice's security controls.

**AMERICAN DENTAL ASSOCIATION TECHNICAL REPORT NO. 1017 FOR ADMINISTRATIVE
PROCEDURES AND THEIR APPLICATION IN DENTISTRY**

CONTENTS

Summary	3
Introduction	5
Purpose	5
Scope	5
Background	6
Administrative Procedures Matrix	8
Where to Begin With Security and Administrative Procedures	9
Practice Impact Analysis	9
Administrative Procedures to Guard Data Integrity, Confidentiality and Availability	12
Certification	13
Chain of Trust Partner Agreement	13
Contingency Planning	13
Formal Mechanism for Processing Records	14
Information Access and Control	14
Internal Audit	18
Personnel Security	19
Security Configuration Management	20
Security Incident Procedures	21
Security Incident Management Process	22
Termination Procedures	24
Security Training	25
What are the Regulation's Major Requirements?	27
What is the Purpose of the Security & Privacy Regulations?	28
What are Security & Privacy Best Practices?	28
What are the Penalties for Non-Compliance with Security & Privacy?	29
Conclusion	30
Additional Information	30
Glossary	31
Reference	34

AMERICAN DENTAL ASSOCIATION TECHNICAL REPORT NO. 1017 FOR ADMINISTRATIVE PROCEDURES AND THEIR APPLICATION IN DENTISTRY

INTRODUCTION

HHS consulted with the American Dental Association throughout the process of developing and promulgating the first national standards for administrative reforms mandated by the 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, 2003;ⁱ
- B Privacy of individually identifiable health information (issued Dec 28, 2000), conformance with the standard by the dentist by April 14, 2004.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, when fully effective in three years, are laws that will require a typical dental practice 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 Provide privacy training to employees;
- D Establish privacy agreements with "business associates";
- E 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 the information conveyed with electronic transactions but is not limited to electronic transactions.^{iv} The new rules are more sweeping than 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.

The development and implementation of administrative procedures are necessary to insure the requirements of privacy are met. All providers should have documented policies for processing health information. Policies should cover both electronic health information and also 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 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 the complex dental environment. The authors hope that the contents of this paper will