

American Dental Association
Technical Report No. 1017

Administrative Procedures and their Application to Dentistry

ADA American
Dental
Association®

2002



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

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 must 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; covered entities must work with their legal staff to address appropriate requirements. This document may serve as a tool to expedite an understanding of the necessary legal actions needed to address requirements, as well as federal and state legislation, as HIPAA has an impact on many aspects of dentistry.

BACKGROUND

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 interpretation.

Best practices suggest health care information that dentists electronically collect, maintain, use or transmit is kept confidential, private and secure. 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.

Who must comply? “Any health care provider, health care clearinghouse, or health plan that electronically maintains or transmits health information pertaining to an individual.” The proposed security standard requires that each health care entity engaged in electronic maintenance or transmission of health information assess potential risks and vulnerabilities to the individual health data in its possession in electronic form and develop, implement and maintain appropriate security measures. Most importantly, these measures must be documented and kept current.^{vi}

This proposed security standard was developed in the spirit of the recommendation that the federal government should work with industry to promote and encourage an informed public debate to determine an appropriate balance between the primary concerns of patients and the information needs of various users of health care information (“...that the security standard development process has been an open one with invitations to a number of organizations to participate in the security discussions”). Although implementation team membership was limited to government employees, non-governmental organizations and business organizations, individuals knowledgeable in security, and educational institutions have been encouraged to express their views.

As a result of the collaborative security regulation development process, the implementation team has chosen to divide the proposed security requirements, for purposes of presentation only, into four Security Categories:

- A Administrative Procedures;
- B Physical Safeguards;
- C Technical Security Mechanisms;
- D Technical Security Services.

This paper will focus on the Administrative Procedure category of Security.^{vii} Administrative procedures to guard data integrity, confidentiality, and availability are documented, formal practices to manage the selection and execution of security measures to protect data and meet the mandated privacy requirements. They also include procedures that describe and document the conduct of personnel in relation to the protection of data.^{viii}

When information is read or copied by someone not authorized to do so, the result is known as loss of confidentiality. When information is modified in unexpected ways, the result is known as loss of integrity. This means that unauthorized changes are made to information, whether by human error or intentional tampering. Information can be erased or become inaccessible, resulting in loss of availability. This means that people who are authorized to get information cannot get what they need. To make information available to those who need it and who can be trusted with it, organizations need to use authentication and authorization. Authorization is the act of determining whether a particular user (or computer system) has the right to carry out a certain activity, such as reading a file or running a program. Authentication is proving that a user is whom he or she claims to be. Authentication and authorization go hand in hand. Users must be authenticated before carrying out the activity they are authorized to perform.^{ix}

A matrix of administrative procedures follows. Each dental practice will need to assess their own specific environment to determine which security procedures they will need to implement in order to meet security policies and requirements.

Matrix of Administrative Procedures

Certification	-----
Chain of trust partner agreement	-----
Contingency plan (all listed implementation features must be implemented).	Applications and data criticality analysis. Data backup plan. Disaster recovery plan. Emergency mode operation plan. Testing and revision.
Formal mechanism for processing records.	-----
Information access control (all listed implementation features must be implemented).	Access authorization. Access establishment. Access modification
Internal audit	-----
Personnel security (all listed implementation features must be implemented).	Assure supervision of maintenance personnel by authorized, knowledgeable person. Maintenance of record of access authorizations. Operating, and in some cases, maintenance personnel have proper access authorization. Personnel clearance procedure. Personnel security policy/procedure. System users, including maintenance personnel, trained in security.
Security configuration mgmt. (all listed implementation features must be implemented).	Documentation. Hardware/software installation & maintenance review and testing for security features. Inventory. Security Testing. Virus checking
Security incident procedures (all listed implementation features must be implemented).	Report procedures. Response procedures.
Security management process (all listed implementation features must be implemented).	Risk analysis. Risk management. Sanction policy. Security policy
Termination procedures (all listed implementation features must be implemented).	Combination locks changed. Removal from access lists. Removal of user account(s). Turn in keys, token or cards that allow access.
Training (all listed implementation features must be implemented)	Awareness training for all personnel (including mgmt). Periodic security reminders. User education concerning virus protection. User education in importance of monitoring logs in success/failure, and how to report discrepancies. User education in password management

WHERE TO BEGIN WITH ADMINISTRATIVE PROCEDURES

Administrative Procedures is the largest category of security issues and relates primarily to policies and procedures in dental practice dealing with the behavioral side of security. Significant input from non-technical resources, such as the American Dental Association, will be required to adequately address potential gaps between current state and future readiness. The dentist should conduct a practice impact analysis, including gap analysis, risk management and risk analysis. The purpose of a practice impact analysis for security is to determine the magnitude of the impact on the practice and to establish the scope of the effort.

Risk Analysis is a process whereby cost effective security/control measures may be selected by balancing the costs of various security control measures against the loss that would be expected if these measures were not in place. The risk analysis can serve as the basis for determining the level of risk deemed acceptable to the dental practice and should drive the review of policy and procedures, as well as the selection process for enhanced security controls. Risk Management is the process of assessing risk, taking steps to reduce risk to an acceptable level and maintaining that level of risk.

A key to compliance is the requirement for complete and current documentation of all security measures in effect. Documentation such as an office procedures manual would include contingency plans, formal records processing and procedures, information access controls, security incident procedures, awareness and training. These should become required reading by employees and always available.^x

PRACTICE IMPACT ANALYSIS

In the process of undertaking this initial analysis a number of the security requirements can be satisfied if appropriately conducted and documented. Following is the Practice Impact Analysis structure. Dental practices should begin by:

- A Developing an awareness program based on the Security and Privacy requirements: This helps gain understanding and support of all office personnel; develop an awareness campaign; and develop a compliance program.
- B Develop leadership and organization: Assign specific individual (s) to be responsible for overall security and privacy issues.
- C Establish a baseline (Baseline Analysis): Determine what types of capabilities are in place today, and what is needed to comply with the regulations.
- D Gap analysis: What are the current security and privacy procedures in place today and those required?
- E Conduct Risk Assessment and Risk Management decisions: Focus on where additional safeguards are needed, and type of safeguards. Determine the risk that you will have a security or privacy breakdown in procedures that you carry on each day, and compare this to the benefit you will gain in better business practices. Develop the best plan to fit your practice. Identify needed resources (dental associations and trading partners) for education and training, software and hardware needs. Are they ready to provide enhanced security and privacy features or information to meet security needs?
- F Policy: This sets responsibility and accountability since only those assigned to office procedures will create a risk. Staff should have access to individual identifiable health information only if their job function

requires such information. Each dental practice must determine who needs access to health information and for what purposes, and document this in their office manual.

- G Documentation: All of the above steps taken to comply with the security and privacy requirements must be documented, signed and dated.

Initial Roles and Responsibilities

The security requirements are very comprehensive and extend far beyond the Information technology environment. Before a practice can start any of its initial security compliance including the business impact analysis, the practice must generate sufficient awareness throughout the office to complete the analysis task and subsequent security activities. Security experts agree that a number of activities to ensure adequate support throughout the enterprise are needed.

Recommended activities for the dental practice include the following:

- A Establish a framework for office buy-in;
- B Develop an awareness program for all affected staff;
- C Establish your security implementation member;
- D Establish security training that is tailored to various staff, agents and contractors.

Smaller or simple practices will have fewer people involved and may undertake their security and privacy activities in a more tailored fashion described by a guide to be developed. A simple environment may consist of:

- A Single site or multiple offices;
- B Independent;
- C Single lead practitioner;
- D Users - 10 or less, likely to have no or low technical experience;
- E Only dial up access to 3rd party networks;
- F One system, multiple applications;
- G 10 or less workstations;
- H One platform, likely Windows;
- I May or may not have existing confidentiality policy (not security);
- J Access control limited by ID and password, lock doors and cabinets;
- K No assigned security or privacy lead.

For example, a simple site may choose to encourage the business/office manager to lead the effort., partner w/IT person (hardware and/or software provider), get hardware and software vendors onboard, and have input from a professional organization such as the ADA.