ADA Technical Report No. 1018
Approval date: January 25, 2005

American Dental Association
Technical Report No. 1018

Technical Security Mechanisms and Their Application to Dentistry

American Dental Association 2005

AMERICAN DENTAL ASSOCIATION TECHNICAL REPORT NO. 1018 FOR TECHNICAL SECURITY MECHANISMS AND THEIR APPLICATION TO DENTISTRY

The Council on Dental Practice of the American Dental Association has approved American Dental Association Technical Report No. 1018 for Technical Security Mechanisms and Their Application to 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. 1018 was confirmed by the ADA SCDI on January 25, 2005.

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. 1018 FOR TECHNICAL SECURITY MECHANISMS AND THEIR APPLICATION TO DENTISTRY

FOREWORD

(This foreword does not form a part of American Dental Association Draft Technical Report No. 1018 for Technical Security Mechanisms and their Application to 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."

Norman Schreiber, HIPAASeminars.com, Phoenix, MD, Chairman of Subcommittee 10 on Dental Informatics Architecture and Devices, prepared this technical report at the request of the ADA Standards Committee on Dental Informatics.

These security measures may not represent requirements of the HIPAA privacy or security regulations. The ADA has developed specific guidance for compliance with HIPAA security regulations. Dentists covered by HIPAA must have complied with HIPAA security regulations by April 21, 2005.

AMERICAN DENTAL ASSOCIATION TECHNICAL REPORT NO. 1018 FOR TECHNICAL SECURITY MECHANISMS AND THEIR APPLICATION TO DENTISTRY

SCOPE

Practitioners need to understand exactly the specific requirements that may be indicated to provide security and how to address each requirement.

While security refers to “ensuring” protection of electronic protected health information (PHI), providers are not expected to implement security protection regardless of the cost. One needs to balance the risks of inappropriate use or disclosure of electronic PHI against the cost of various protective measures.

The size and capabilities of the provider also may be taken into account. Smaller practices will not be expected to implement the levels of security in the same manner and at the same cost as a large entity, since risk and vulnerability increase with size and complexity of practice. Small practices tend to be less complex entities, have less sophisticated technology, have fewer resources to expend on security, and may have a lower risk of inappropriate use and disclosure of electronic PHI as a result of having a smaller staff.

This report discusses requirements for small practices to ensure transmission security to protect the integrity of data sent over the Internet and to authenticate the data received.

This document may provide information regarding legal implications of the security and privacy regulations. This document does not provide legal advice, and 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 security and privacy has an impact on many aspects of dentistry.

SCALABILITY OF SECURITY PRACTICES

Security for the protection of electronic PHI provides an entity flexibility to adopt and implement measures that are appropriate for that particular entity. This means that a small practice will not need to take the same measures to comply with the security of this information as will a large practice, clinic or hospital. In deciding which security measures to adopt, a provider must consider the following factors:

A The size, complexity and capabilities of the entity;

B The entity’s technical infrastructure, hardware and software security capabilities;

C The costs of security measures; and

D The probability and degree of potential harm from risks to electronic PHI.

SECURITY RISK ANALYSIS: A REVIEW[i]

Security Risk Analysis is deciding what needs attention in order to secure information. The first step is analysis. A security policy deals with both the “what” and the “how.” That is, it deals with what needs to be protected and the type of protection. Therefore, these two questions must be considered during the analysis:

A What is one going to protect?

B Where is one vulnerable?