ADA Technical Report No. 1020
Approval date: February 13, 2003

American Dental Association
Technical Report No. 1020

Physical Safeguards and Applications to Dentistry

ADA American Dental Association 2003

AMERICAN DENTAL ASSOCIATION TECHNICAL REPORT NO. 1020 FOR PHYSICAL SAFEGUARDS AND APPLICATIONS TO DENTISTRY

The Council on Dental Practice of the American Dental Association has approved American Dental Association Technical Report No. 1020 for Physical Safeguards and Applications 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. 1020 was confirmed by the ADA SCDI on February 13, 2003.

The ADA SCDI thanks Norman Schreiber D. D. S., 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. 1020 FOR PHYSICAL SAFEGUARDS AND APPLICATIONS TO DENTISTRY

FOREWORD

(This foreword does not form a part of the American Dental Association Draft Technical Report No. 1020 for Physical Safeguards and Applications 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 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, D.D.S. SCDI Working Group 10.3 prepared this report at the request of SCDI Subcommittee 10 for Dental Informatics Architecture and Devices (Dr. Scott Trapp, Chairman).

AMERICAN DENTAL ASSOCIATION TECHNICAL REPORT NO. 1020 FOR PHYSICAL SAFEGUARDS AND APPLICATIONS TO DENTISTRY

CONTENTS

AMERICAN DENTAL ASSOCIATION TECHNICAL REPORT NO. 1020 FOR PHYSICAL SAFEGUARDS AND APPLICATIONS TO DENTISTRY

SUMMARY

This technical report will provide the dentist information on physical safeguards to guard data integrity, privacy, confidentiality, and availability and how they apply to dentistry to provide for assigned security responsibility, media controls, physical access controls, and policy/guideline on workstation use, secure workstation location, and security awareness training.

In order to administer their programs, the Department of Health and Human Services, other Federal agencies, State Medicaid agencies, private health plans, health care providers, and health care clearinghouses must assure their customers (such as patients, insured, providers, and health care plans) that the confidentiality and privacy of health care information they electronically collect, maintain, use, or transmit is secure. Security of health information is especially important when health information can be directly linked to an individual.[iii]

With the exception of the security portion, the HIPAA Law should apply to each health care provider when transmitting or receiving any of the specified electronic transactions. The security regulation would apply to each health care provider electronically maintaining or transmitting any health information pertaining to an individual. [iv]

The security standard is applicable to all health care information electronically maintained or used in an electronic transmission, regardless of format (standard transaction or a proprietary format); no distinction is made between internal corporate entity communication or communication external to the corporate entity.[v]

The requirements and implementation features for physical safeguards are presented in a matrix of the proposed Security rule. Each of these safeguards is required to be documented. This documentation is to be made available to those individuals responsible for implementing the safeguards and to be reviewed and updated periodically.

Some universities and companies have developed methods for security of their networked computer systems and have documented these, however they have neither the scope nor the extent required by the new SECURITY AND PRIVACY law.[vi]

The following matrix depicts the requirements and implementation features for the Physical Safeguards category. [vii]

Physical Safeguards to Guard Data Integrity, Confidentiality and Availability

REQUIREMENT	**IMPLEMENTATION**
Assigned security responsibility	
Media controls (all listed implementation features must be implemented).	Access control. Accountability (tracking mechanism). Data backup. Data storage. Disposal.
Physical access controls (limited access) (all listed implementation features must be implemented).	Disaster recovery. Emergency mode operation. Equipment control (into and out of site). Facility security plan. Procedures for verifying access authorizations prior to physical access. Maintenance records. Need-to-know procedures for personnel access. Sign-in for visitors and escort, if appropriate. Testing and revision.
Policy/guideline on work station use	
Secure work station location	
Security awareness training	

AMERICAN DENTAL ASSOCIATION TECHNICAL REPORT NO. 1020 FOR PHYSICAL SAFEGUARDS AND APPLICATIONS TO DENTISTRY

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 environments within the context of the security and privacy regulations. The need to maintain the privacy of Individually Identifiable Health Information (IIHI) and Protected Health Information (PHI) during the processes of treatment. payment and healthcare operations is paramount. 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 for operational implementations of security and privacy requirements. 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 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.

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 security policy requirements and their interpretation are subject to possible change; however, it is best to develop the ability to satisfy the required implementation features of the Security Notice of Public Rulemaking (NPRM)

WHERE TO BEGIN WITH PHYSICAL SAFEGUARDS TO GUARD DATA INTEGRITY, PRIVACY, CONFIDENTIALITY AND AVAILABILITY

Physical safeguards to guard data integrity, privacy, confidentiality, and availability are intended to provide for protection of computer systems and media. They provide for assigned security responsibility, media controls, physical access controls, and policy/guideline on workstation use, secure workstation location, and security awareness training.

As with other security measures, physical security controls and safeguards could be selected if they are cost-beneficial. This does not mean that a user must conduct a detailed cost-benefit analysis for the selection of every control. There are general ways to justify the selection of controls, especially in situations where the cost is insignificant, but the benefit is material. A good example of this is a facility with a key-locked low traffic door to a restricted access area. The cost of keeping the door locked is minimal, but there is a significant benefit.