American Dental Association
Technical Report No. 1021

Data Integrity, Redundancy, Storage and Accessibility

ADA® American Dental Association 2005

AMERICAN DENTAL ASSOCIATION TECHNICAL REPORT NO. 1021 FOR DATA INTEGRITY, REDUNDANCY, STORAGE AND ACCESSIBILITY

The Council on Dental Practice of the American Dental Association has approved American Dental Association Technical Report No. 1021 For Data Integrity, Redundancy, Storage and Accessibility. 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. 1021 was confirmed by the ADA SCDI on January 25, 2005.

The ADA SCDI thanks Scott Benjamin, Advanced Integration & Mentoring, Inc., Hancock, NY, as chairman of Working Group 10.4 for Data Redundancy for leading the development effort.

AMERICAN DENTAL ASSOCIATION TECHNICAL REPORT NO. 1021 FOR DATA INTEGRITY, REDUNDANCY, STORAGE AND ACCESSIBILITY

FOREWORD

(This foreword does not form a part of American Dental Association Technical Report No. 1021 for Data Integrity, Redundancy, Storage and Accessibility).

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 10.4 for Data Redundancy. The SCDI Working Group chairman is Scott Benjamin. SCDI Working Group 10.4 prepared this report at the request of SCDI Subcommittee 10 for Dental Informatics Architecture and Devices (Norman Schreiber, Chairman).

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. 1021 FOR DATA INTEGRITY, REDUNDANCY, STORAGE AND ACCESSIBILITY

SCOPE

This report reviews options presently available to prevent data loss and corruption, maintain data integrity and restore and maintain access to data (backup); noting their effects on a dental facility's standard operating procedures. It also discusses appropriate contingency plans in emergency situations for recovery and authentication (verification) of the data as well as accessing the information. This report does not address security issues as related to privacy/confidentially of health information. These issues are discussed in ADA Technical Report No's. 1016, 1017, 1018, 1019, 1020 and 1031.[1-6]

The accumulation and recording of data by electronic means offer a degree of accuracy and security unavailable by any other mechanism when the proper protocol is followed on a routine and consistent basis. A dental practice's data protection plan needs to address every possible situation to protect the data that has been collected and recorded. Therefore, this plan needs to have separate steps and protocols to address all of the potential causes of data loss or corruption. The recommendations provided herein are designed to be technology-neutral and to be scalable to address the needs of both large and small dental facilities.

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.

TYPES OF POTENTIAL FAILURES OF DATA INTEGRITY AND AVAILABILITY

The first step in addressing this issue is the identification of the possible reasons for the loss or corruption of, or access to, electronic data. Each facility needs to understand these issues and establish the appropriate protocol to protect themselves from these situations. Table 1 shows an outline of the major areas of concern and exposure in this area.

Table 1. Types of Potential Failure of Loss of Electronic Information.

	Type of Failure	Examples
1	Hardware Failure	Storage Device Failure Hardware Functionally (non storage device failure) Power Failure
2	Software Program Corruption/ Failure	Software Applications Corruption/ Failure Operating Systems Corruption/ Failure Networking Systems Corruption/ Failure Virus Infections, Malware, Spyware
3	Software Data Loss/Corruption	Corruption of Data Deletion of Data
4	Physical Damage of System	Fire Vandalism Natural Disaster, Etc.