ADA Technical Report No. 1096
Approved by ADA SCDI: July 18, 2018

American Dental Association

**Technical Report No. 1096**

# Electronic Protected Health Information HIPAA Security Risk Analysis

ADA American Dental Association®

**Standards Committee on Dental Informatics**

**2018**

# AMERICAN DENTAL ASSOCIATION TECHNICAL REPORT NO. 1096 FOR ELECTRONIC PROTECTED HEALTH INFORMATION HIPAA SECURITY RISK ANALYSIS

The ADA Standards Committee on Dental Informatics (SCDI) has approved American Dental Association Technical Report No. 1096 for Electronic Protected Health Information HIPAA Security Risk Analysis. Working Groups of the ADA SCDI formulate this and other specifications and technical reports 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. The ADA SCDI confirmed approval of ADA Technical Report No. 1088 on July 18, 2018.

The SCDI thanks the members of Working Group 10.3, Dental Information Systems Security and Safeguards, and the organizations with which they were affiliated at the time the technical report was developed:
Mary Licking (chairman), Nashua, NH;
John R. Anderson, Battle Ground, WA;
Deborah J. Carr, Christmas, FL;
Mohamed Harunani, Texas City, Texas; and
Linda Harvey, Jacksonville, FL.

# AMERICAN DENTAL ASSOCIATION TECHNICAL REPORT NO. 1096 FOR ELECTRONIC PROTECTED HEALTH INFORMATION HIPAA SECURITY RISK ANALYSIS

## FOREWORD

(This Foreword does not form a part of ADA Technical Report No. 1096 for Electronic Protected Health Information HIPAA Security Risk Analysis).

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:

> *The ADA SCDI shall develop informatics standards, specifications, technical reports and guidelines and interact with other entities involved in the development of health informatics standards aimed at implementation across the dental profession.*

Although certain commercial entities, equipment, or materials may be identified in this document in order to describe a procedure or concept adequately, such identification is not intended to imply recommendation or endorsement by ADA, or the authors of the Technical Report, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

This document may provide information regarding legal implications of the HIPAA security and privacy regulations and may serve as a tool to expedite an understanding of the necessary actions needed to address requirements. However, this document does not provide legal advice, and individual covered entities must work with their legal advisers to address the actions needed to address the requirements in each case.

ADA TECHNICAL REPORT NO. 1096 FOR ELECTRONIC PROTECTED HEALTH INFORMATION HIPAA SECURITY RISK ANALYSIS

INTRODUCTION

In contemporary dental practice, technology is the heart of most operations. As more and more dental offices are going paperless, there is a corresponding expansion of information that is stored or transferred electronically, thus increasing the potential or threat of a breach. Performing a risk analysis is an essential first step, a primary regulation and tends to mitigate federal and civil monetary risk.

According to the FBI estimates, there were an estimated 4000 ransomware attacks in 2016. Dental practices are considered "soft" or easy targets and have become a prime target for these attacks. Dental offices collect a goldmine of information, including payor and guarantor information, medical and dental history and various demographic information. The financial and reputational impact of ransomware attacks, or a breach of any kind, can cripple or bankrupt a practice and have a negative impact on all the entities involved, including the patient. In the modern world the largest asset of any practice or company is its data, so it is imperative that all persons and practices secure and protect their data.

The purpose of this document is to assist covered practitioners in fulfilling their legally mandated obligation to conduct a security risk analysis, develop a plan to protect patient data privacy and security and to train the dental team. In doing so, the document will help covered entities to understand and analyze the risk, and assist in choosing the appropriate partners in the fields (in terms of vendors of software and/or services) in order to help train and protect all the parties involved.

This document does not address an "assessment," which is the term the Office of Civil Rights gives to the investigation conducted after a breach or potential breach has occurred.

There are basically four rules that were passed and that apply in this area. The last one passed in 2013 and while many covered dental entities may consider this a hardship or burden, it can also be a guide to assist covered dental entities in protecting their most import asset – their data and access to it. Protection of the data and compliance with HIPAA guidelines can help minimize or prevent direct and indirect business loss due to any potential breach or loss of access.

The Healthcare Insurance Portability and Accountability Act (HIPAA, 1996) established the baseline requirements for preserving the overall confidentiality of protected health information (PHI). HIPAA specifically requires covered entities to:

- Protect individuals' health records (all formats) and other individually identifiable health information created, maintained, received by or on behalf of covered entities and their business associates;
- Protect individuals' PHI by regulating the circumstances under which covered entities may use and disclose protected health information;
- Have contracts or other arrangements in place with business associates that perform functions for, or provide services to, or on behalf of, the covered entity;
- Grant individual rights with respect to their protected health information, including rights to examine and obtain a copy of their health records and to request corrections.

The Security Rule (2003 enacted, 2005 compliance required) established national standards to protect individuals' electronic personal health information that is created, received, transmitted, used, or maintained by a covered entity. The Security Rule specifically requires covered entities to:

- Implement specific administrative, physical, and technical safeguards to protect health information; and
- Maintain contracts with their business associates stating that the business associates will also appropriately safeguard the electronic protected health information they receive, create, maintain, or transmit on behalf of the covered entities.