Revised ADA Technical Report No. 1096
All Interested Parties Review: November 2022

Proposed Revision of American Dental Association
Technical Report No. 1096

Electronic Protected Health Information HIPAA Security Risk Analysis

ADA American Dental Association®

Standards Committee on Dental Informatics

2022

PROPOSED REVISED 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 the proposed revision 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.

This technical report was prepared by SCDI Working Group 10.3 for Dental Information Systems Security and Safeguards. . The chairman of SCDI Working Group 10.3 is Mary Licking. SCDI Working Group 10.3 prepared this report at the request of Jonathan Knapp, chairman, SCDI Subcommittee on Information Exchange.

PROPOSED REVISED AMERICAN DENTAL ASSOCIATION 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.

The Health Information Technology for Economic and Clinical Health (HITECH, 2009) stimulated the growth of the electronic health record and implemented security provisions. HITECH strengthened privacy and security protections by establishing:

- Four categories of violations that reflect increasing levels of culpability;
- Four corresponding tiers of penalty amounts that significantly increase the minimum penalty amount for each violation; and
- A maximum penalty amount of $1.5 million for all violations of an identical provision per each calendar year. [In November, 2021, that $1.5 million figure, with the inflation adjustments applied, became $1,806,757. Source: Alder, Steve, What are the penalties for HIPAA Violations, accessed on 01.31.2022 at www.hipaajournal.com]

The **HIPAA Omnibus Rule (2013)** is comprised of a set of final regulations modifying the Health Insurance Portability and Accountability Act (HIPAA) Privacy, Security, and Enforcement Rules. It officially implemented several provisions of the Health Information Technology for Economic and Clinical Health (HITECH) Act:

- Expanded individual rights to access of their protected health information electronically;
- Set new limits on how information can be used and disclosed for marketing and fundraising purposes, and prohibited the sale of an individuals' health information without their permission;
- Amended the breach notification final rule with a requirement to determine the breach's "risk of compromise," rather than harm;
- Included ALL digital and non-digital data or communication in PHI; including verbal.

According to a U.S. Government interagency report, on average there were 4,000 daily ransomware attacks since early 2016 (hhs.gov).

SCOPE

The scope of Proposed ADA Technical Report No. 1096 for Electronic Protected Health Information HIPAA Security Risk Analysis is to:

- Review the fundamental concepts and terminology of the Health Insurance Portability and Accountability Act (HIPAA), Security Rule, Health Information for Economical Data Risk Analysis such as Sections 160.103 (definitions), 164.306 (General Rule), 164.308 (Administrative Guideline), 164.310 (Physical Guidelines), 164.312 (Technical), 164.502 (definitions), 164.514 (Uses and Disclosures including Minimally Necessary),

and 164.530 (Administrative Requirements) located in 45 Code of Federal Regulations. This review will provide a foundation for beginning a Patient Data Risk Analysis.

- Highlight the steps needed to start a Patient Data Security Risk Analysis which should include:
  1. Review of organizational and educational tasks; and
  2. Development and implementation of a HIPAA privacy compliance program.
- Outline the steps required in a risk management plan as described in § 164.306 (B) follow-up and should include:
  1. Itemization of forms and notices the privacy and security standards require;
  2. Identification of business associates;
  3. Inventory of existing policies and procedures at the corporate, institutional, and departmental levels, and the training;
  4. Development of HIPAA-specific policies and procedures, inventory of information assets including hardware/software and connectivity;
- Recommend Patient Data Security Risk Analysis tools

DEFINITIONS

Analysis – A detailed examination (for the purpose of this TR this is pre-breach)

Assessment – the act of judging or deciding (for the purpose of this TR this is post-breach)

Administrative Safeguards – are defined in the Security Rule as the “administrative actions and policies, and procedures to manage the selection, development, implementation, and maintenance of security measures to protect protected health information and to manage the conduct of the covered entity's workforce in relation to the protection of that information.” (164.304) Among other important items, this includes workforce training.

Breach – A breach is the acquisition, access, use or disclosure of protected health information in a manner that compromises the privacy or security or poses a significant risk of financial, reputational, or other harm to one or more individuals. A breach is presumed unless a covered dental entity or business associate can demonstrate that there was a low probability of harm.

Health and Human Services which oversees the Office of Civil Rights (OCR) recently ruled that a cyber-attack on an information system is considered a reportable offense, unless the practice can demonstrate the low probability that an impermissible disclosure of PHI was made. In accordance with 45 C.F.R. 164.402(2) the practice and or their business associates are required to notify HHS of the incident. The burden of proof lies with the covered dental entity or business associate. See www.hhs.gov

Business Associate – A Business Associate is defined as (45 C.F.R 160.103):

(1) A Health Information Organization, E-prescribing Gateway, or other person that provides data transmission services with respect to protected health information to a covered entity and that requires access on a routine basis to such protected health information.
(2) A person that offers a personal health record to one or more individuals on behalf of a covered entity.

(3) A subcontractor that creates, receives, maintains, or transmits protected health information on behalf of the business associate." See Guidance Document at www.hhs.gov

Covered Entity – A Covered Entity is defined as (45 C.F.R. 160.103): (1) A health plan.

(2) A health care clearinghouse.

(3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter

Cyber Attack – A cyber attack is any type of offensive maneuver employed by nation-states, individuals, groups, or organizations that targets computer information systems, infrastructures, computer networks, and/or personal computer devices by various means of malicious acts usually originating from an anonymous source that either steals, alters, or destroys a specified target by hacking into a susceptible system. These can be labelled as either a cyber campaign, cyber-warfare or cyberterrorism in different context. Cyberattacks can range from installing spyware on a PC to attempts to destroy the infrastructure of entire nations. Cyberattacks have become increasingly sophisticated and dangerous as recent malware occurrences have demonstrated significant impact on healthcare institutions. User behavioral analytics and Security Information and Event Management (SIEM) are used to identify these attacks. Legal experts are seeking to limit use of the term to incidents causing physical damage, distinguishing it from the more routine data breaches and broader hacking activities

ePHI – Electronic Protected Health Information

ID – Identification

IT – Information Technology

Malware – Malicious Software

Minimally Necessary – As defined in C.F.R. 45 164.502(b)(1): When using or disclosing protected health information or when requesting protected health information from another covered entity or business associate, a covered entity or business associate must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

Mitigation – The act of mitigating, or lessening the force or intensity of something unpleasant, as wrath, pain, grief, or extreme circumstances

Physical Safeguards – are defined as the "physical measures, policies, and procedures to protect a covered entity's information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion."

Ransomware – malware planted illegally in a computer or mobile device that disables its operation or access to its data until the owner or operator pays to regain control or access.

Technical Safeguards – are defined as the "the technology and the policy and procedures for its use that protect electronic protected health information and control access to it." This includes back up protocols.

Threat – A *threat* is any circumstance or event with the potential to adversely affect or cause harm to assets, operations and individuals via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service.

Vulnerability – is a weakness, whether administrative or technical, which allows an attacker to reduce a system's information assurance and exploit a threat.

UNDERSTANDING THE RISK

Practices and/or organizations should consider their core mission, business functions, business processes, business segments, common infrastructure, support services, vendor information, any proprietary information and their information systems in general when performing an analysis and estimating how a breach could negatively affect them. A Risk analysis (45. CFR 164.308(a)(1)(ii)(A (Required) is a detailed examination and evaluation of potential risk that could adversely impact a practice.

Conducting a risk analysis involves careful examination of vulnerabilities and threats that, when exploited, may result in harm to the patient and/or the covered dental entity. It entails the process of identifying assets, determining potential risks, existing safeguards, and the potential impact arising from the misuse or inappropriate application of the information or information systems. An objective risk analysis is foundational to implementing a security management plan (45. CFR 164.308(a)(1)(ii)(B).

A risk analysis provides definitive information for decision makers to guide and inform responses to information security risks and is not a one-time activity. A covered dental entity should conduct a risk analysis on an ongoing basis as part of its risk management plan. There is not a set frequency defined in the rule, however a risk analysis should be conducted on a periodic basis, or when there has been physical changes or changes in either processes, equipment, vendor relationships or the law.

It is important for practices and organizations to remember that they are ultimately responsible for their data and how their data is created, stored and transmitted. A risk analysis is a business decision, *not* an IT decision. **There is a misconception that the practice management or electronic health record provider is responsible for maintaining the security of the data. This is a false narrative and could result in severe penalties for the practice.** It is important to remember that practice management and imaging software providers and other supporting providers are Business Associates. Frequently, practices and organizations are under the impression that this responsibility has been transferred to the IT company or department; this is not true unless specifically contracted out. Too often there is a disparity between the services that are actually being provided by the IT company or department and exactly what the expectations are. This disparity is a risk that could result in severe penalties.

WHAT ARE THE REQUIREMENTS OF THE LAW – CODE 45 OF FEDERAL REGULATIONS SECTIONS 160.103, 164.306,164.308, 164.310, 164.312, 164,501, 164.502, 164.514, AND 164.530?

It is important to understand the definition in section 160.103 and how they apply to the practices or the organizations business processes and operations. It also considers that covered entities, in the normal course of business, carry out administrative and financial activities.

According to 164.306 Covered entities and business associates must:

(1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.
(2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.

(3) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part.

(4) Ensure compliance with this subpart by its workforce.

The law mandates that a thorough examination (Analysis) be conducted to determine potential risks and vulnerabilities to the confidentiality, integrity, and availability of protected health information held by a covered dental entity and/or their vendors either directly or indirectly. Security works within what is known as the CIA (Confidentiality, Integrity, and Availability) Triad. The information should always be confidential and only be seen by people who absolutely need to see the information. The information should also be correct and accurate and any changes to the information are made by people who are authorized to make such changes. The information should also be readily available when authorized individuals need to access the data. Practices and organizations are required by 164.308 to: "Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered dental entity or business associate.” This requirement is the first mandate under the Administrative Safeguards.

Covered dental entities are required to designate a security official, in addition to the privacy officer, who is responsible for developing and implementing policies and to "lead" the covered dental entity in achieving HIPAA/HITECH compliance. In small practices this may be the doctor or someone the doctor delegates to this task. In larger organizations there may be an individual that is tasked solely with these responsibilities. This individual needs to be trained in and have a solid understanding of the HIPAA/HITECH Rule and how to protect patient data. (164.308(2)

When conducting a risk analysis, the required and addressable paragraphs, 164.308 (Administrative Safeguards), 164.310 (Physical Safeguards), and 164.312 (Technical Safeguards) should be reviewed and addressed. The risk analysis should:

- Identify where PHI is stored, received, maintained or transmitted (desktop, laptop, removable drives, etc.);
- Identify and document potential threats and vulnerabilities (theft, fire, flood, loss, etc.);
- Evaluate current security measures used to safeguard PHI (password, backup, physical locks, encryption, etc.);
- Assess whether the current security measures are used properly;
- Determine the likelihood of a “reasonably anticipated” threat;
- Assign risk levels for vulnerability and impact combinations;
- Determine the potential impact of a breach of PHI (High, Medium, or Low to your practice);
- Document the analysis and take action where necessary;
- Document mitigation.

There are several definitions that must be known and accepted when conducting a risk analysis under 164.501. This section is rather lengthy, however, key definitions are:

- *Designated record set* – A group of records that are created, transmitted or stored by or for a covered entity; includes data involving diagnosis, treatment decisions, billing, payment and anything else that involves making decisions regarding the individual patient/s.

- *Direct Treatment Relationship* – Any treatment relationship between an individual patient and a healthcare provider that is not indirect treatment.

- *Indirect Treatment Relationship*– means a relationship between an individual and a health care provider in which:

  (1) The health care provider delivers health care to the individual based on the orders of another health care provider;

  and

  (2) The health care provider typically provides services or products, or reports the diagnosis or results associated with the health care, directly to another health care provider, who provides the services or products or reports to the individual.

- *Financial remuneration* – This definition involves all activities taken by covered dental entities to obtain either direct or indirect payment including but not limited to claim information provided to benefit providers.

- *Treatment* – is the provision, coordination or management of healthcare by one or more providers including consultation between providers directly relating to a specific patient?

The goal is to keep patient information as private and secure as possible, however there are times when information needs to be released or shared. The guidelines for general use and disclosure under 164.502 and the guidelines for other uses and disclosures under 164.514, also see the minimally necessary section in 164.514.

PREPARING FOR A RISK ANALYSIS

When preparing for a risk analysis, remember that the Security Rule does not mandate any specific methodology or format; the Rule provides the flexibility to tailor the concepts of a risk analysis to the covered dental entity. It is important is to understand the HIPAA fundamental framework and its essential purposes. The scope and expectation of the risk analysis should also be defined, as there are key elements that should be part of any comprehensive risk analysis.

Start the preparations by identifying the individual(s) in your covered dental entity that will participate in the risk analysis. For example, will this be an individual or a work group and will it include the practice owner(s), Security Officer, Privacy Officer, Office Manager, IT vendor or IT employee, outside consultant or attorney? Depending upon the size of the covered dental entity, the dentist and the team may overlap in duties in the work group.

CONDUCTING THE RISK ANALYSIS

The objective of this step is to produce a list of data/information security risks that can be prioritized by risk level and be used to make risk response decisions. To accomplish this objective, the covered dental entity must understand and analyze the various threats and vulnerabilities, impacts and likelihood, and the uncertainty associated with the risk and thus the risk analysis process.

First, create an inventory by identifying and categorizing the assets of all the media, both onsite and offsite, that contains protected health information. Identify all the devices in the covered dental entity that store patient information, including but not limited to, the server, portable backup drives, outdated workstations, tablets, fax and copy machines with scanning capability, mobile devices and/or personal cell phones.

Next, identify PHI that is kept remotely, such as but not limited to: cloud storage companies, old backup storage devices, off-site storage devices and outdated servers or workstations that may be stored at an offsite facility such as a private residence or a self-storage unit. (45 C.F.R. §§ 164.308(a)(1)(ii)(A) and 164.316(b)(1).)Part of this inventory process includes identifying who has access to these devices and the data contained on these devices. Data workflows should be mapped from initial patient contact through data collection, diagnosis, treatment, billing and payment operations, so that the covered dental entity knows exactly who has access to PHI and to insure the minimally necessary rule is followed.

IDENTIFY POTENTIAL VULNERABILITIES AND THREATS

Identify any reasonably anticipated vulnerabilities and threats and those that are unique to the work environment that could lead to an incident or event that could compromise the safety and security of protected health information. 45 C.F.R. §§
164.306(a)(2), 164.308(a)(1)(ii)(A), 164.316(b)(1)(ii). and 164.316(b)(1)(ii).

REVIEW CURRENT SECURITY MEASURES

Review and assess all security measures currently in place to safeguard PHI, as required. The Security Rule dictates that a covered dental entity must have reasonable and appropriate safeguards in place to protect patient protected health information.

These safeguards include:

- Administrative Safeguards 164.308
- Workforce training and oversight
- Workforce termination procedures
- Sanction policy
- Disaster Plan
- Periodic security risk analysis

- Physical Safeguards 164.310
- Facility access controls
- Workstation Use
- Data Backup
- Computer and device equipment

- Technical Safeguards 164.312
- Unique User ID
- Encryption
- Auto log off
- Access Controls

- Organizational Requirements 164.314
- Business Associates Agreements

- Written Policies 164.316

- Written policies and procedures safeguarding patient information
- Documentation of security measures
- Periodic updates

DETERMINE THE LIKELIHOOD OF THE OCCURRENCE OR EVENT AND THE IMPACT

This step involves identifying and documenting all reasonable vulnerabilities and anticipating the possible threats that are unique to the work environment. Also determine that, if such a vulnerability or threat was to occur, what the impact would be and would it result in impermissible access or disclosure of PHI. 45 C.F.R. §§ 164.306(a)(2) and 164.316(b)(1)(ii). 45 C.F.R. §§ 164.308(a)(1)(ii)(A) and 164.316(b)(1)(ii).)

MANAGEMENT PLAN 164.308(a)(1)(ii)(B)

The results of the risk analysis should clearly identify existing safeguards and, more importantly, any areas where safeguards are insufficient or lacking. This risk analysis is the foundation for developing and implementing a risk management plan, as required. A risk management plan involves prioritizing, evaluating and implementing the appropriate risk-reducing controls or safeguards that result from the risk assessment process. This may involve consideration of new security products or programs. It may also require changes of workflows or processes and perhaps changes of business associates, business practices or even vendors.

Every covered dental entity should have written security policies that are specific to their facility and, for multi-site organizations, a specific plan for each site. (CFR 45§ 164.308). These policies should reflect practice or site-specific policies and procedures to prevent, detect, contain, and correct security violations.

Once policies are developed, implementation should start with staff training. A successful security program may involve changes in work flows, processes and behaviors. This should be done for the whole team initially and for all new additions to the team. To insure consistency, training also is essential. The human factor often is the biggest risk factor; one that can only be minimized by a comprehensive and robust training program. 45 C.F.R. § 164.308(a)(3) & (4); [18] 45 C.F.R. § 164.308(a)(5)(i); [19] 45 C.F.R. § 164.308(a)(1)(ii)

In addition, 45 C.F.R. § 164.308(a)(5) requires periodic retraining whenever environmental or operational changes affect the security of ePHI. Changes may include: new or updated policies and procedures; new or upgraded software or hardware; new security technology; or even changes in the Security Rule.

The Security Awareness and Training standard has four implementation specifications:

- Security reminders;
- Protection from malicious software;
- Log-in monitoring;
- Password management criteria.

RISK ANALYSIS RESOURCES

As indicated throughout this document, the rule allows for flexibility and does not dictate a specific manner to conduct a risk analysis; it only states that an analysis must be conducted. The Office of Civil Rights has issued a guide for conducting a risk analysis which contains a "Myths and Facts" section. It notes that a checklist is a useful tool but falls short of performing a "systematic" risk analysis. The same document *reminds small providers that they are not exempt and must complete a risk analysis.* It also indicates that it is not necessary to outsource a risk analysis. The document states, "It is possible for small practices to do risk analysis themselves using self-help tools. However, doing a thorough and professional risk analysis that will stand up to a compliance review will require expert knowledge that could be obtained through services of an experienced outside professional."

Several options for conducting a risk analysis include:

- HIPAA Security Risk Assessment Tool by HHS;
- Online tools;
- An objective independent expert, such as a certified consultant or expert. State, Federal and other agencies exist to provide certifications; verify certifications with the applicable certifying body.

BIBLIOGRAPHY

Risk assessment

1. https://www.healthit.gov ~~[accessed August 26, 2016.]~~ [accessed September 18, 2022].

2. http://www.ahima.org, to access the document: Apple, G. and Brandt, M., Ready, Set, Assess! An Action Plan for Conducting a HIPAA Privacy Risk Assessment [accessed August 26, 2016].

3. http://www.ahima.org, to access the document: Greenhalgh, T., Navigating the New HIPAA Safe Harbor, July 2021 [accessed February 9, 2022].

Laws and legislation

1. E-Government Act [includes FISMA] (P.L. 107-347), December 2002.

2. Federal Information Security Management Act (P.L. 107-347, Title III), December 2002.

3. HITECH Act Amendment, P.L. 116-321, January 2021.

4. Cybersecurity Information Sharing Act (CISA), P.L. 114-113, December, 2015. This act is part of the Cybersecurity Act of 2015.

5. Coronavirus Aid, Relief, and Economic Security (CARES Act), P. L. 116-136, H.R. 748, 116th Congress, March 2020.

6. 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program, May 2020, effective 06/30/2020. [This is how the title appears in the Federal Register]. A summary of the final rule: [Official website of the Office of the National Coordinator for Health Information Technology – https://healthit.gov/topic/onc-cures-act-final-rule]. Alternatively, go to https://healthit.gov then click on topics, then click on Laws, Regulation, and Policy, then on the screen that appears – in the left hand column, click on ONC's Cures Act Final Rule.

Policies, directives, instructions

1. Office of Management and Budget, Circular A-130, Appendix III, Transmittal Memorandum #4, Management of Federal

Information Resources, November 2000.

2. Committee on National Security Systems Instruction (CNSSI) No. 4009, National Information Assurance (IA) Glossary, April

2010.

3. Committee on National Security Systems Instruction (CNSSI) No. 1253, Security Categorization and Control Selection for

National Security Systems, March 2012.

4. Department of Homeland Security Federal Continuity Directive 2 (FCD 2), Federal Executive Branch Mission Essential

Function and Primary Mission Essential Function Identification and Submission Process, February 2008.

Standards

1. National Institute of Standards and Technology Federal Information Processing Standards Publication 199, Standards for

Security Categorization of Federal Information and Information Systems, February 2004.

2. National Institute of Standards and Technology Federal Information Processing Standards Publication 200, Minimum Security

Requirements for Federal Information and Information Systems, March 2006.

3. ISO/IEC 31000:2009, Risk management – Principles and guidelines.

4. ISO/IEC 30101:2009, Risk management – Risk assessment techniques.

5. ISO/IEC Guide 73, Risk management – Vocabulary.

6. ISO/IEC 27005:2011, Information technology – Security techniques – Information security risk management.

Guidelines

1. National Institute of Standards and Technology Special Publication 800-66 Revision 1, An Introductory ---Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule October 2008

2. National Institute of Standards and Technology Special Publication 800-30 Revision 1 Guide for Conducting Risk Assessments – September 2012

3. National Institute of Standards and Technology – Framework for Improving Critical Infrastructure Cybersecurity – February 2014

4. National Institute of Standards and Technology Special Publication 800-18, Revision 1, Guide for Developing Security Plans for Federal Information Systems, February 2006.

5. National Institute of Standards and Technology Special Publication 800-34, Revision 1, Contingency Planning Guide for Federal Information Systems, May 2010.

6. National Institute of Standards and Technology Special Publication 800-37, Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, February 2010.

7. National Institute of Standards and Technology Special Publication 800-39, Managing Information Security Risk: Organization, Mission, and Information System View, March 2011.

8. National Institute of Standards and Technology Special Publication 800-53, Revision 3 5, Security and Privacy Controls for Information Systems and Organizations, August, 2017.

9. National Institute of Standards and Technology Special Publication 800-53A, Revision 1, Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans, June 2010.

10. National Institute of Standards and Technology Special Publication 800-59, Guideline for Identifying an Information System as a National Security System, August 2003.

11. National Institute of Standards and Technology Special Publication 800-60, Revision 1, Guide for Mapping Types of Information and Information Systems to Security Categories, August 2008.

12. National Institute of Standards and Technology Special Publication 800-64, Revision 2, Security Considerations in the System Development Life Cycle, October 2008.

13. National Institute of Standards and Technology Special Publication 800-65, Integrating IT Security into the Capital Planning and Investment Control Process, January 2005.

14. National Institute of Standards and Technology Special Publication 800-70, Revision 2, National Checklist Program for IT Products--Guidelines for Checklist Users and Developers, February 2011.

15. National Institute of Standards and Technology Special Publication 800-117, Version 1.0, Guide to Adopting and Using the Security Content Automation Protocol (SCAP), July 2010.

16. U. S. Government, Interagency (fourteen [14] agencies), How to Protect Your Networks from Ransomware: Technical Guidance Document, Undated.

17. “Final Guidance on Risk Analysis”, hhs.gov/hipaa/for-professionals/security/guidance/final-guidance-risk-analysis/index.html (accessed February 1, 2022). Once at hhs.gov, type into the search bar, hipaa, then click on the link, “hipaa for professionals”, then type into the search bar, risk analysis, then click on the link, final guidance on risk analysis.

18. Cybersecurity Act of 2015, Section 405(d), P.L. 114-113, December 2015. To access the four-part series on Cybersecurity Best Practices that are indicated by the HITECH Act Amendment of January 5th, 2021: Healthsectorcouncil.org, click on About, click on Task Groups, under the header, Section 405(d)-Health Industry Cybersecurity Practices, scroll down for links to the entries: 1) Main document [Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (HICP)], 2) Technical Volume 1: Cybersecurity Practices for Small Health Care Organizations, 3) Technical Volume 2: Cybersecurity Practices for Medium and Large Health Care Organizations, and 4) Resources and Templates. Alternatively, the four volumes mentioned above can be found at: https://405d.hhs.gov/resources

19. National Institute of Standards and Technology, White Paper: Framework Improving Critical Infrastructure Cybersecurity, Version 1.1, nist.gov, 04/16/2018. Note: This entry is an update to the entry at 3.on the list, **Guidelines,** an entry that is dated with the year, 2014**.**

ADA American Dental Association®
America's leading advocate for oral health

211 East Chicago Avenue, Chicago, Illinois 60611
T 312.440.2500   F 312.440.7494   www.ada.org