Proposed Revision of American Dental Association
Technical Report No. 1021

Data Integrity, Redundancy, Storage and Accessibility

ADA American Dental Association®

2022

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

FOREWORD

(This Foreword does not form a part of the proposed revision 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 10.3 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.

These security measures may not represent requirements of the HIPAA privacy or security regulations. TheADA 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~~. Dentists covered by Health Insurance Portability and Accountability Act (HIPAA) must have complied with HIPAA security regulations by dates described at hhs.gov

PROPOSED REVISED 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.. 1018. .[1]

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.

DEFINITION OF TITLE TERMS

The four terms in the title of this technical report are defined below. The terms as mentioned in the title are: Data Integrity, Redundancy, Storage and Accessibility.

Data Integrity — Integrity is the property that data or information have not been altered or destroyed in an unauthorized manner (Code of Federal Regulations, Title 45, Section 164.304).

Data redundancy – Occurs when the same piece of data is stored in two or more places (Alley, G., alooma.com, click on blog, accessed 02.09.22)

Data storage – Essentially means that files and documents are recorded digitally and saved in a storage system for future use (cdw.com accessed 02.09.22).

Data accessibility – *D*ata access refers to the ability to or the means to read, write, modify, or communicate data, information or otherwise use any system resource. Note: this definition refers to the meaning of access in Code of Federal Regulations (C.F.R.) Title 45, Subtitle A, Subchapter C, Part 164, Subpart C. This definition does not apply to Subparts D and E. For more on how the term, access, is used in those Subparts, please see those subparts. Generally, Subpart D discusses breaches and Subpart E addresses the right to access records.

Availability, as given in the title of the section, "Types of Potential Failures of Data Integrity and Availability", in this technical report is defined below.

Availability – The ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource (45 C.F.R. Section 164-304 Definitions).

Under **BIBLIOGRAPHY**, under the subheader, Definition of Title Terms, see the six (6) entries.

The Environment for Data Integrity, Redundancy, Storage, and Accessibility: An Observation

Zarour, M. et al, commented on a trend in healthcare that contributes to risk, "A study on various healthcare service providers shows that 85% of devices in medical organizations are using and running on outdated operating system or infrastructure [protenus.com]. This kind of situation develops an open path for attackers to exploit vulnerabilities and harm the healthcare sector effectively."

Under **BIBLIOGRAPHY**, under the subheader, **The Environment for Data Integrity, Redundancy, Storage, and Accessibility: An Observation**, see the two entries.

Data Integrity, a 2022 Update

The United States government has addressed data integrity by publishing documents that serve as guidance on the subject. See the **BIBLIOGRAPHY** section, subheader, **Guidance** for a list of six documents by the National Institute of Standards and Technology (NIST) related to data integrity.

One recent paper offered remarks on the availability of scholarly documentation on data integrity. (Zarour, M., et al, June 2021 that was referred to above) provides two quotes that are telling regarding the current state of data integrity reports in healthcare: 1) "While data integrity management of healthcare is the most critical and demanding subject for modern security scientists and scholars, authors have also noticed that there is not much literature…on the healthcare data integrity issues," and 2) "The results of the [systematic literature review] strongly indicate that the healthcare sector needs a new and more robust data integrity approach."

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
3	Software Data Loss/Corruption	Corruption of Data Deletion of Data
4	Physical Damage of System	Fire Vandalis m

MAJOR CONCERNS IN FORMULATING A DATA INTEGRITY AND REDUNDANCY PLAN

Once an office has developed an understanding of the potential causes of data loss and the problems they present, practitioners must formulate a data integrity and redundancy plan that is comprehensive and appropriate to insure that all data is safe, and that the facility can continue to function in an acceptable manner addressing all the patients' needs.

When formulating a data protection, redundancy and archiving plan, three basic areas of concern need to be addressed and accounted for; each with a specific and unique function. These three areas are:

A Long term archiving;
B Provisional or short term redundancy;
C Immediate protection.

Long Term Archiving

The function of long term archiving is to provide permanent data storage on a stable media that only is used once (such as CD or DVD), of a write once read many (WORM) nature, and which can be retrieved over an extended period with a time-stamped copy of the data. Long-term archived records should be a part of the dental entity's permanent records. The permanent business records are usually stored offsite in a location such as a safe deposit box, or with the practice's attorney.

Provisional or Short Term Redundancy

Provisional records are designed to store electronic information for an extended period until the long-term archive is updated. The media used for this function is often reusable for a period of time (such as tapes, CD- RW, re-writable DVD and removable hard drives). Their basic function is to provide temporary redundant storage that can retain several generations or re-visions of the electronic information and allow retrieval of information that may be required in the event of a failure or corruption in the system. Provisional records on removable media also provide for offsite protection of data and electronic information.

Immediate Protection

Immediate protection is designed to protect data and configuration information in the event of a hardware failure, primarily a failure of the hard drive or primary data storage. Appropriate configurations allow the dental entity to continue to function in a contingency mode, with minimal or no interruptions and no loss of data. A RAID- configured hard drive is a form of immediate protection.

FORMULATING A DATA INTEGRITY AND REDUNDANCY PLAN

The steps that should be included when formulating and implementing an electronic data integrity and redundancy plan include the following:

- Needs assessment (risks analysis);
- Hardware and software requirements;
- Consumable supplies required;
- Storage plans for archived data;
- Cost analysis;
- Formulating disaster recovery plan;
- Formulation of written documentation of procedures for electronic data integrity and redundancy (backup and restore plan);
- Training.

Needs Assessment (Risks Analysis)

To evaluate the dental facility's needs, the practitioner must identify the potential risks, vulnerabilities and requirements for the insuring that the practice's and patient's records remain complete. The practitioner needs to address concerns over how, or if, electronic data can be recovered if lost. The type of redundancy needed is directly related to this issue. This data critical analysis should address all of the information that is being recorded electronically regardless of whether the information is financial or health related. This information includes text, images and other graphical data. Other considerations include time sensitivity, the need for immediate accessibility of the data and whether a hard copy of the data exists, in either paper or film form. The items to consider when doing the risk analysis for a dental facility follow:

A Determination of the data to be protected — formal assessment of the type of electronic information collected (Data critical analysis):
  - Health and dental information data (text);
  - Financial data;
  - Images (radiographs, photographs, etc.);
  - Other graphical data (periodontal charting etc.).

B Need for immediate, short term and long term (archive) accessibility;

C Is there a "hard" copy of the data;

D Ability to recreate the electronic data;

E Amount of data;

F Location of data;

G Time sensitivity;

H Type of redundancy required by data;

I Storage of media and data (long and short term).

For more on how to develop a risk analysis, see: ADA (American Dental Association) Technical Report Number 1096 for Electronic Protected Health Information HIPAA Security Risk Analysis, 2018.

Hardware and Software Requirements

When formulating the data redundancy and archiving protection plan, the dental facility needs to consider the hardware and software required to achieve the required protection. The more critical the data that is acquired, the more sophisticated the hardware and software that is required. The hardware and software should allow automation of the process as much as possible to reduce the possibility of human error or incorrect administration of the process.

The proper selection and use of software operating systems, applications, and utility programs can help

prevent corruption and corresponding data loss before it occurs. The office must implement appropriate antivirus and firewall hardware and software to assist in keeping data from being corrupted.

Listed below are some of the hardware types that should be considered as part of an office redundancy and archiving armamentarium:

- Tape drive;
- CD-recorder (often referred as a CD burner);
- DVD-recorder (often referred to as a DVD burner);
- RAID controller (allows data to be stored on multiple disks at same time);
- Multiple hard drives (provides multiple places for data to be stored);
- Removable hard drives (allows for large amounts of data to be stored outside computer);
- Internet storage service;
- UPS (Uninterruptible Power Supply);
- Surge suppressor;
- Hardware firewall.

Table 2 displays the various types of storage media available for backing up and storing data with their capacities and relative speeds.

Software considerations for redundancy and archiving include the application software that performs the backup and restore functions. This software should have the ability to: verify that the process was successful; catalogue the media sets; compress the data to minimize storage space required; and perform the necessary maintenance utilities for the backup application.

Verification, though adding extra time to the total backup, is extremely important. After backing up files to the media, the backup software goes back to make sure they are readable. If backup tapes are used, this process can identify aging tapes. This function can help discover when the tapes are becoming unreliable – before it's too late. Although this option should not be used instead of occasional test restores, it can give a little more piece of mind.

Compression is extremely valuable and desirable to reduce the size (megabytes) of the media sets. One aspect to be aware of is that most image management software compresses the image as much as possible (without losing data) before being saved initially. This means that image files will have minimal (if any) reduction in file size.

Cost Analysis

The practice should evaluate the cost and effectiveness of the entire data integrity and redundancy plan. This measure is required to insure that appropriate funds are budgeted to obtain appropriate data protection. The value of protection cannot be understated and corners must not be cut.

Formulation of Disaster Recovery Plan

Each dental entity needs to establish Standard (daily) Operating Procedures (SOP) to insure the electronic information is protected.

Table 2. Storage Media Types.

Device	Media	Speed	Comments
3.5" Floppy	1.44 MB Removable	Slow	Nice for very small amounts of data. Cheap and portable media. Not practical for most dental
CD-R/W	Up to 700 MB Removable Media	Moderate	Most dental practices will require many disks for comprehensive backups. Some media is “write once read many” format (WORM) and except
DVD-R/W, DVD+R	Up to 4.7 GB Removable Media	Moderate to Fast	Similar to CD-R/W but with even greater storage space. Some Media is a Write Once Read Many Format (WORM) and is today's desired media for
Flash Media	Up to multiple GBs and	Fast	Many different formats available, with USB interface being the most common. Is most often
Hard Drive (Primary)	Presently up to 300 GB and growing.	Fast	Good for recovering files, but not good for total system failures since the original and backup data are on the same physical device. (If there is more than one computer networked together, data can
Hard Drive(Alternate)	Up to 300 GB and growing.	Fast	If the drive is removable it can be physically disconnected from the computer/network as a form of protection when not backing up files and can be removed from premises for off site storage.
ZIP® Drive	100 MB or 250 MB	Slow	The most popular high-capacity floppy-disk type device, but still too small for most dental
Tape Drive	4GB to 110 GB	Fast	A high-capacity removable media. Generally used by more sophisticated users. Must use archiving or backup/restore software to write or retrieve
Remote Backup or Internet Backup	Unlimited storage available	Moderate-depends on internet	No devices to handle. Need an Internet connection — the faster and more stable the connection the better. Often initial upload of data is done with other media (tape/DVD/ hard drive etc). Data is off-site. There are ongoing fees for service. Costs
Printer	Unlimited	Very Slow	A paper backup is better than nothing at all.

These procedures need to include the following aspects:

- What information is to be protected;
- How the information is to be protected;
- Who is responsible (accountable) for verifying the successful archiving (backup);
- Emergency mode operation plan;
- Restoration plan and procedures;
- Testing and revision;
- Training.

Formulation of Written Documentation of Procedures

After formulation of the required procedures, the dental entity needs to develop a written plan. The dental entity should plan to update/revise it annually, or when significant changes to the electronic data system have occurred or needs have changed. Items to be included in the documentation are:

- Training procedures & training records;
- Daily maintenance procedures;

- Validation of redundancy (backup);
- Validation of equipment/hardware functionality;
- Log (backup records).

The office also should have a written Contingency Plan (disaster recovery protocol) of the procedures to be followed in the event of an incident. In the event of a disaster incident, a log should be made showing the actions taken.

Daily maintenance records should include the information that was archived (backup), the mechanisms used, the location of the backup (data) set, and any unusual incident, failure, or discrepancies that may have occurred during the backup process.

Training

A very important part of the data integrity and backup plan is training. The office staff should be trained in all aspects of the entity's data protection plan. Training must include knowledge of how to restore and operate in a contingency mode. A good practice is to set up a restore schedule to an alternate system to insure the procedures are correct and that that the backup is valid and restorable.

BACKUP AND REDUNDANCY: TECHNICAL PRACTICES AND PROCEDURES

Any electronic dental record considered as health information is required to have redundancy (backup copies). The type and nature of the redundancy is dependent on the nature and other forms of the record. Any electronic dental record that cannot be reproduced from a hard copy format (paper, film, photograph, etc.) must have a form of immediate data redundancy (often referred to as RAID protection or data mirroring), so that the data is recorded simultaneously on at least two separate storage devices (hard drives, etc.). These devices (disks) should be equipped with a failure notification alarm, and the capability of continuing to access data while operating in a contingency mode with minimal or no interruption. The dental facility also needs to be able to function in a contingency mode, using auxiliary hardware, in the event of a failure of the primary computer hardware.

Additional archiving (redundancy) needs to be performed on a daily basis. The data should be stored off-site by electronic transmission to the remote location, or copying to a removable storage medium (such as tape, CD, DVD, removable hard drive etc.).

Types of Backup

There are common options in nearly every backup software program, the most common of which are; Normal (usually referred to as "Full"), Differential, and Incremental. Microsoft Windows Backup also provides two other choices: Daily and Copy. To understand how these backup types differ, one needs to know something about file "attributes." Attributes are settings, sometimes called "bits" or "flags," that are part of each system file. The
concept of file attributes dates all the way back to the earliest DOS days and attributes are still used to mark files today. Many attributes exist that can be set on a file, but the most commonly used attributes include:

- **R** - marking the files as read only;
- **S** - marking the file as a system/secret file;
- **H** - marking the file as hidden;
- **A** - marking the file as ready for archiving.

When a file is changed in any way – even just renamed – the "A" attribute is set, or "turned on." This indicates that the file has changed since the last time it was backed up. During a normal backup, this

attribute will be "turned off."

Full Backup

A full backup is simply backing up all files on the system. Users may choose to update archive attributes if they plan on doing incremental or differential partial backups. There are three types of full file backups. These are described in Table 3.

Table 3. Types of Full Backup.

Types of Full	Description	st devices for this Application	Comments
Entire System (Image-	Protects the entire system – usually takes more time and larger capacity backup devices, but it provides a smooth	CD-R/W DVD-	Also great for making copies of
Entire System (File-	Protects the entire system with a file-based technique. Combines system recovery and file restoration from the	CD-R/W DVD-	Best of both worlds.
Data Files Only	Limits the backups to just the critical files gives the essential protection needed and gives the broadest options	ALL Devices Ideal for Remote Backup	Initial setup takes a little time, but saves

Incremental Backup

An incremental backup backs up only the files modified since the last backup. When running an incremental backup, users need to update the archive attribute while backing up only modified files. Often the incremental backups are appended to the full backup set. The result is a tape with the changes that occurred daily. This type of backup is useful if the user wishes to have an audit trail of file usage activity on their system and will enable them to restore a specific day's work without restoring any changes made since that point in time. To do a full restore for four days after a full backup, he must restore the full backup and all four data sets after it.

Differential Backup

A differential backup type is similar to incremental, in that it backs up only files that have the Archive bit turned on. It differs in that after backing files up, it leaves the Archive turned on. The list of files grows each day until the next full backup is performed, clearing the archive attributes This means that files that have been changed will be backed up during each differential backup until either a normal or incremental backup is performed to turn the Archive bit off. This backup takes the same or somewhat longer time than an incremental backup, but is much
easier to restore from. In order to do a full system restore, the user would install the operating system first and then restore only the files from the most recent differential backup. If a normal backup was performed, the user would restore the files from that backup and then restore from the most recent differential backup.

Daily Backup

The daily backup type is like a differential off-shoot. In this backup type, only files that were changed (have the Archive bit on) during the current day are backed up, and the Archive bit is left unchanged. This backup type is not generally used as part of a recovery program, because one would need to do a normal backup and then a daily backup from each and every day since the normal backup in order to do a full system restore.

Copy Backup

A copy type of backup is similar to a normal backup, except that it leaves the Archive bit unchanged. This backup type can be used to back up any selected files, regardless of whether or not the Archive bit is turned on. This will leave the Archive bit the same as before the backup. This is most commonly used between normal and incremental backups.

Scheduled vs. Manual Backups

Scheduled backups allow backups to be performed automatically with minimal or no user involvement at a selected time or time interval. This automation will minimize user error and help to insure proper redundancy. Manual backup means that the backup is administered and run in an attended mode.

Rewritable Media Rotation

If re-writable media is being for daily archiving, dental offices are recommended to use a scheduled rotation of multiple media sets (multiple tapes or optical media) to create copies (generations) of the data. The Grandparent, Parent, Child technique is a simple method that is accomplished by labeling the rewritable media sets by the day of the week. A different media set would be labeled for each Friday in the month and for each month of the year. Labeling for this technique would look like the following:

MONDAY TUESDAY WEDNESDAY THURSDAY FRIDAY1
MONDAY TUESDAY WEDNESDAY THURSDAY FRIDAY2
MONDAY TUESDAY WEDNESDAY THURSDAY FRIDAY3
MONDAY TUESDAY WEDNESDAY THURSDAY MONTH1

MONDAY TUESDAY WEDNESDAY THURSDAY FRIDAY1
MONDAY TUESDAY WEDNESDAY THURSDAY FRIDAY2
MONDAY TUESDAY WEDNESDAY THURSDAY FRIDAY3
MONDAY TUESDAY WEDNESDAY THURSDAY MONTH2

MONDAY TUESDAY WEDNESDAY THURSDAY FRIDAY1
MONDAY TUESDAY WEDNESDAY THURSDAY FRIDAY2
MONDAY TUESDAY WEDNESDAY THURSDAY FRIDAY3
MONDAY TUESDAY WEDNESDAY THURSDAY FRIDAY4
MONDAY TUESDAY WEDNESDAY THURSDAY MONTH3, etc.

Because some months have more than four weeks, it will take more than 20 media sets for regular backups for one full year.

The permanent archiving of the data onto a long lasting stable storage media (such as an optical type media, i.e., CD or DVD) with a Write Once Read Many (WORM) format should be completed on a quarterly basis at minimum. These new media sets should be identifiable by the manufacturer's unique serial number for each individual piece of media (disk). The archiving should be documented by logging the following information:

A Date of archiving;

B Description of electronic information that was archived:
- Operating system used;
- Archiving method;
- Program name(s);
- Dates of data (health information) contained in media;

C Type of media used (brand of media and serial number of media);

D Number of media sets made;
E Number of copies made;
F Storage location of copies (media);
- At least one copy must be stored off site;
- An additional copy should be stored on site;

G Personnel or organization that recorded and authenticated the media.

Non-Critical/Reproducible Data

Though the electronic archiving of any electronic dental record that can be reproduced from a hard copy format (paper, film, photograph, etc.) is not as critical, dental facilities still are recommended to follow the previously described protocol for archiving data for non-reproducible records. Though immediate redundancy (RAID protection) is not mandatory, dental facilities are strongly encouraged to engage in this practice, which can be very beneficial.

Offices also are encouraged to execute the permanent archiving of this data on a long lasting stable storage media (such as an optical media type, i.e., CD or DVD, etc.) with a Write Once Read Many (WORM) format.

Off-Site Data Backup

Off-site storage of copies of the electronic data is required for the data is to be truly secure. Investing in and meticulously adhering to a regular data backup schedule will not help if all the data backup copies are in one place and that place is struck by disaster such as fire, theft, or a natural disaster.

Dental facilities are advisable to keep an electronic copy (preferably DVDs or CDs) of the media set data in security boxes at banks. Some practitioners also keep an additional copy of the data at the home in a secure HIPAA compliant manner.

Remote / Internet Backup and Archiving

Remote backup is very similar to regular backup, with one important difference. Instead of sending backups to
media attached to a local computer, remote backup works by sending data to another secure computer safely off-site. Using both a local backup system and a remote backup system offers the best of both worlds. Critical files, including all health information, images, financial files and databases can be kept on the remote backup system, while the local backup system can be used to create a full backup of the entire file system (including program files) at regular intervals.

Most remote systems can encrypt the data prior to transmission to the offsite backup server. HIPAA compliant encryption technology and a user-defined password (encryption key) ensure that nobody, including employees of the remote site, can access the data. Remote systems that do not technically encrypt the data can still securely transmit the data using a secure tunneling protocol to the secure server site. The data is securely protected before it leaves the local facility.

A remote backup system can be fully automated once it has been configured. Time, frequency, list of files, and file types to be backed up are saved in the client (practice's) software. Then the actual backup can take place automatically on the set schedule. The remote back ups work similarly to local backups, usually occurring at night while the office is closed. Because the systems can be fully automated no expenses are incurred for personnel to perform, monitor and verify the backup process.

The amount of data, its compression, and the speed of the Internet connection will determine the length

of time for the backup. Backups can be incremental – archiving only files that have changed since the previous backup
– or full, to backup all of all critical data. The use of cable modems or DSL connections are recommended to speed up the process but are not required. An initial backup and all full backups will take the longest because these require transmission of all data files in the backup set to the offsite storage and not just the data that has recently changed. Some vendors recommend or may even require that the initial data be sent (transferred) by other mechanisms such as tape, DVD, or removable hard drive.

Restoring in the event of a catastrophic loss from a remote storage site can be very problematic due to the amount of data that may need to be transferred and the bandwidth available. This situation should be thoroughly investigated before deciding that a remote backup system should be the primary archiving system or only a part of the plan.

If archiving health Information is only being done by off site recording, with no on site hard (paper etc.) or electronic copy of the records) by a third party vendor (Application Service Provider or ASP), considerations for the following situations should be addressed and planned for:

- System failure;
- Discontinuance of business;
- Discontinuance of business relationship;
- Any other unforeseen problem.

The issue of the patient's and health care provider's access to permanent health information data in a readable format needs to be addressed before any health information is handled/stored in this manner.

The provider (dental facility) is advised to house (store) a copy of the all the health information data records (or a real time copy) on site along with the appropriate application necessary to view and append this data as needed
and required. The provider is further advised to archive the data with the appropriate measures to insure both redundancy and access to the data as required by the nature of the data. This allows the application program to be maintained and updated by the ASP on the Internet and still insures that the data is always accessible to the patient and health care provider.

Data Redundancy – 2022 Update

The American Dental Association / American National Standards Institute has addressed data redundancy and backup by publishing a document that serves as guidance in an area that is not addressed in the legacy document, in cloud computing. The United States government has published guidance on data protection and loss prevention that was posted online in 2021 that addresses redundancy and backup. These two documents are listed in the BIBLIOGRAPHY section, under **Guidance**, under the subheader, Documents related to redundancy and backup. Also in the BIBLIOGRAPHY section, see the two entries under subheader, Laws and legislation.

Data Storage – 2022 Update

The American Dental Association / American National Standards Institute has addressed data storage by publishing a document that serves as guidance in an area that is not addressed in the legacy document, in cloud computing. The United States government has published guidances on the data storage topics of media sanitization, security for storage infrastructure, securing Picture Archiving and Communication System (PACS) cybersecurity for the healthcare sector, and on information technology asset management. These five documents are listed in the BIBLIOGRAPHY section, under **Guidance**, under

the subheader, Documents related to storage and archiving, and that includes the cloud computing document mentioned above. Also in the BIBLIOGRAPHY section, see the two entries under subheader, Laws and legislation.

Data Accessibility – 2022 Update

The American Dental Association / American National Standards Institute has addressed data accessibility by publishing a document that serves as guidance in an area that is not addressed in the legacy document, in cloud computing. The United States government has published a guidance on the data accessibility topic of attribute-based access control.

These data accessibility documents are listed in the BIBLIOGRAPHY section, under **Guidance**, under the subheader, Documents related to accessibility.

SUMMARY

The accumulation and recording of data by electronic means offers a degree of accuracy and security not available 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 any situation that can possibly arise to protect all the data that has been collected and recorded, both clinically and administratively, from any patient encounter, to address all the potential causes of data loss or corruption. The best defense against such a disaster is a proper data integrity, redundancy, storage and accessibility protection plan. Creating, investing in and meticulously adhering to a well thought-out system, which includes archiving and backing up all the dental entity's data regularly and properly, will allow dental practices to advance to a higher level of technical sophistication, productivity, efficiency and quality of care.

LEGACY REFERENCES

1. American Dental Association Technical Report No. 1016: Electronic/digital signature uses in dentistry. Chicago: American Dental Association, 2003

2. American Dental Association Technical Report No. 1017: Administrative Procedures and Their Application in Dentistry. Chicago: American Dental Association, 2002

3. American Dental Association Technical Report No. 1018: Technical Security Mechanisms and Their Application to Dentistry. Chicago: American Dental Association, 2005

4. American Dental Association Technical Report No. 1019: Technical Security Services and Their Application to Dentistry. Chicago: American Dental Association, 2003

5. American Dental Association Technical Report No. 1020: Physical Safeguards and Their Application to Dentistry. Chicago: American Dental Association, 2003

6. American Dental Association Technical Report No. 1031: Internet Security Issues for Dental Information Systems. Chicago: American Dental Association, 2004

BIBLIOGRAPHY [2022 Update]

Definition of Title Terms
https://www.ncbi.nlm.nih.gov Zarour, M., Alenezi, M., Ansari, M., Pandey, A., Ahmad, M., Agrawal, A., Kumar, R., and Khan, R., Health Technology Letter, Ensuring Data Integrity of Healthcare Information in the Era of Digital Health, June 2021, accessed 02.09.2022

alooma.com, click on blog, Alley, G., What is data redundancy, accessed 02.09.2022

cdw.com, What is data storage? Data storage types & attributes, accessed 02.09.2022

45 Code of Federal Regulations 164-304, Subpart C, accessed 9.21.2022

45 Code of Federal Regulations, Part 164, Subpart D, accessed 9.21.2022

45 Code of Federal Regulations, Part 164, Subpart E, accessed 9.21.2022

The Environment for Data Integrity, Redundancy, Storage, and Accessibility: An Observation
https://www.ncbi.nlm.nih.gov Zarour, M., Alenezi, M., Ansari, M., Pandey, A., Ahmad, M., Agrawal, A., Kumar, R., and Khan, R., Health Technology Letter, Ensuring Data Integrity of Healthcare Information in the Era of Digital Health, June 2021.

https://www.protenus.com/press/press- release/breached- patient- record- tripled- in- 2018- vs- 2017- as- health- data- security- challenges- worsen. Accessed 3 Oct 2020 [access was performed by Zarour et al].

Major Concerns in Formulating a Data Integrity And Redundancy Plan
ADA Technical Report Number 1096 for Electronic Protected Health Information HIPAA Security Risk Analysis, 2018.

Laws and legislation
Cybersecurity Act of 2015, Section 405(d), P.L. 114-113, December 2015. To access the four-part series on the Cybersecurity Best Practices that was inspired by the Cybersecurity Act of 2015, Section 405(d), and is 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, click on 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

Guidance

Documents related to data integrity

nist.gov, NIST SP 1800-11 Data Integrity: Recovering from Ransomware and Other Destructive Events, September 22, 2020.

nist.gov, NIST SP 1800-25 Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events, December 2020

nist.gov, NIST SP 1800-26 Data Integrity: Detecting and Responding to Ransomware and Other Destructive Events, December 2020

nist.gov, NIST White Paper (Draft) Securing Data Integrity Against Ransomware

nist.gov, NIST Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0, February 2014

nist.gov, NIST White Paper, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, April 2018

Note: SP refers to Special Publication. For more on NIST references, see nist.gov

Documents related to redundancy and backup

ada.org, ADA (American Dental Association) Technical Report Number 1091, Cloud Computing: Implications and Recommendations for Dental Practice 2018, reaffirmed February 2021.

https://405d.hhs.gov/resources (accessed 9.21.22) Technical Volume 2: Cybersecurity Practices for Medium and Large Healthcare Organizations [note especially the section within it: Cybersecurity Practice 4: Data Protection and Loss Prevention], December 01, 2021; This is a resource provided by the Cybersecurity Act of 2015, Section 405(d).

Documents related to storage and archiving

ada.org, ADA Technical Report Number 1091, Cloud Computing: Implications and Recommendations for Dental Practice, 2018, reaffirmed February 2021.

nist.gov, NIST SP 800-209 Security Guidelines for Storage Infrastructure, October 2020.

nist.gov, NIST SP 1800-5 IT Asset Management, September 2015. Note: IT means information technology.

nist.gov, NIST SP 1800-24 Securing Pictures Archiving and Communication Systems (PACS) Cybersecurity for the Healthcare Sector, December, 2020

https://405d.hhs.gov/resources Technical Volume 2: Cybersecurity Practices for Medium and Large Healthcare Organizations [note especially the section within it: Cybersecurity Practice #5: IT Asset Management] December 01, 2021; This is a resource provided by the Cybersecurity Act of 2015, Section 495(d). Note: IT means information technology.

Document related to accessibility

ada.org, ADA Technical Report Number 1091, Cloud Computing: Implications and Recommendations for Dental Practice, 2018, reaffirmed February 2021.

nist.gov, NIST SP 800-162 Guide to Attribute Based Access Control (ABAC) Definition and Considerations, August 2019

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