Designation: E2682 – 09 (Reapproved 2014)

Standard Guide for Developing a Disaster Recovery Plan for Medical Transcription Departments and Businesses[1]

This standard is issued under the fixed designation E2682; the number immediately following the designation indicates the year of original adoption or, in the case of revision, the year of last revision. A number in parentheses indicates the year of last reapproval. A superscript epsilon (ε) indicates an editorial change since the last revision or reapproval.

1. Scope

1.1 This guide applies across multiple medical transcription settings in which healthcare documents are generated and stored: medical transcription departments, home offices, and medical transcription service organizations (MTSOs). Currently there is no standard disaster recovery plan in the medical transcription industry to provide guidelines for individuals, departments, and businesses to use for designing a disaster recovery plan for their medical transcription environment.

1.2 A disaster is when a sudden event brings great damage, loss, destruction, or interruption of critical services. These guidelines could assist in developing an organized response to reduce the time for loss of services, maintain continuity of workflow, and speed the overall business recovery process.

1.3 This guide supports the HIPAA Security Rule for ensuring data integrity with a contingency plan to include a data backup plan, a disaster recovery plan, and an emergency mode operational plan.[2]

1.4 This guide is consistent with the requirement for disaster planning and recovery procedures as stated in Guide E1959.

1.5 This guide is not intended as a disaster recovery plan for Health Information Management Departments or for an entire healthcare facility.

2. Referenced Documents

2.1 *ASTM Standards:*[3]

E1869 Guide for Confidentiality, Privacy, Access, and Data Security Principles for Health Information Including Electronic Health Records

E1959 Guide for Requests for Proposals Regarding Medical Transcription Services for Healthcare Institutions

2.2 *Other Documents:*

Public Law 104-191 Health Insurance Portability and Accountability Act of 1996 (HIPAA)[2]

45 CFR Part 142 Security and Electronic Signature Standards[4]

3. Terminology

3.1 *Definitions:*

3.1.1 *author, n*—the person originating content for a healthcare document.

3.1.2 *backups, n*—retrievable, exact copies of data. The primary method for ensuring that organizations can recover from a system crash or disaster.[5]

3.1.3 *confidential, adj*—status accorded to data or information indicating that it is sensitive for some reason, and therefore, it needs to be protected against theft, disclosure, or improper use, or a combination thereof, and must be disseminated only to authorized individuals or organizations with a need to know. **E1869**

3.1.4 *confidentiality, n*—the property that information is not made available or disclosed to unauthorized individuals, entities, or processes. **45 CFR Part 142**

3.1.5 *contingency plan, n*—an alternate way of doing business when established routines are disrupted.[5]

3.1.6 *disaster, n*—a sudden event bringing great damage, loss, destruction or interruption of critical services.

3.1.7 *individually identifiable health information, n*—any information, including demographic information collected from an individual, that *(1)* is created or received by a health care provider, health plan, employer, or health care clearinghouse; and *(2)* relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, and

[1] This guide is under the jurisdiction of ASTM Committee E31 on Healthcare Informatics and is the direct responsibility of Subcommittee E31.15 on Healthcare Information Capture and Documentation.

Current edition approved June 1, 2014. Published July 2014. Originally approved in 2009. Last previous edition approved in 2009 as E2682- 09. DOI: 10.1520/E2682-09R14.

[2] Available from U.S. Government Printing Office Superintendent of Documents, 732 N. Capitol St., NW, Mail Stop: SDE, Washington, DC 20401. See also http://aspe.hhs.gov/admnsimp.

[3] For referenced ASTM standards, visit the ASTM website, www.astm.org, or contact ASTM Customer Service at service@astm.org. For *Annual Book of ASTM Standards* volume information, refer to the standard's Document Summary page on the ASTM website.

[4] Available from the U.S. Department of Health & Human Services, 200 Independence Avenue, S.W., Washington, D.C., 20201, www.hhs.gov.

[5] Medical Records Disaster Planning, A Health Information Manager's Survival Guide, AHIMA, Chicago, IL.

(i) identifies the individual, or *(ii)* with respect to which there is a reasonable basis to believe that the information can be used to identify the individual. **Public Law 104-191, Section 1171 (6)**

3.1.8 *privacy, n*—the right of an individual to be left alone and to be protected against physical or psychological invasion or misuse of their property. It includes freedom from intrusion or observation into one's private affairs, the right to maintain control over certain personal information, and the freedom to act without outside interference. **E1869**

3.1.9 *provider, n*—a business entity which furnishes health care to a consumer; it includes a professionally licensed practitioner who is authorized to operate a healthcare delivery system. **E1869**

3.1.10 *secure environment, n*—free from access by unauthorized persons and from unauthorized or accidental alteration.

3.1.11 *security, n*—encompasses all of the safeguards in an information system, including hardware, software, personnel policies, information practice policies, disaster preparedness, and the oversight of all these areas. The purpose is to protect both the system and the information it contains from unauthorized access from without and from misuse from within. **45 CFR Part 142**

3.2 *Acronyms:*

3.2.1 *HIPAA*—Health Insurance Portability and Accountability Act

3.2.2 *MT*—medical transcriptionist

3.2.3 *MTSO*—medical transcription service organization

4. Significance and Use

4.1 This guide acknowledges the importance of a well-designed disaster recovery plan that will protect health information and business information from damage, minimize disruption, ensure integrity of data, and provide for orderly recovery.

4.2 This guide suggests methods to protect the confidentiality and security of healthcare documentation during a disaster.

4.3 It is intended that this guide will contribute to compliance with laws and regulations to improve protection of health information documentation and data integrity with the development of the contingency plan requirement.

4.4 This guide will explain key points to include in preparing a disaster recovery plan to resume operations and minimize losses due to unscheduled interruption of critical services if a disaster would occur.

4.5 This guide is intended to assist in the development of appropriate policies and procedures that provide protection for individually identifiable health information in a secure environment in the event of a disaster.

5. Elements of Disaster Recovery Planning

NOTE 1—Disaster recovery planning includes the identification of key components of a disaster recovery plan, gathering the necessary information to provide the details to tailor the plan to meet the organization's needs, formalization and approval of the disaster recovery plan, annual testing of the implementation of the requisite disaster recovery action, and formal review and necessary revision of the disaster recovery plan.

5.1 Activation of Response Plan:[6]

5.1.1 Policy Statement:

5.1.1.1 To ensure that the plan is effective and that all involved understand its purpose, there must be a clearly defined policy statement. This statement should define the scope and overall objectives of the plan.

5.1.2 Table of Contents.

5.1.3 Introduction:

5.1.3.1 Use of the document.

5.1.3.2 How it is to be revised.

5.1.3.3 Training requirements.

5.1.3.4 Exercise and testing schedules.

5.1.3.5 Plan maintenance schedule.

5.1.3.6 Roles and responsibilities.

5.1.3.7 General information about the facility.

5.1.3.8 Compliance with federal, state, local, and health regulatory agencies.

5.1.4 Emergency Information Sheet:

5.1.4.1 Fire/police departments.

5.1.4.2 Hospitals.

5.1.4.3 Emergency shut-off.

5.1.4.4 Utility companies.

5.1.4.5 Other agencies needed for an emergency.

5.1.4.6 Telephone/reporting tree.

5.1.4.7 List of assistance/equipment vendors.

5.1.5 Resource Priorities:

5.1.5.1 Personnel.

5.1.5.2 Records.

5.1.5.3 Technology.

5.1.6 Plan Activation with Response Outline:

5.1.6.1 Lead personnel responsibilities.

5.1.6.2 Assessing the situation.

5.1.6.3 Organizing/prioritizing efforts.

5.1.6.4 Establishing a command post.

5.1.6.5 Eliminating hazards.

5.1.6.6 Controlling the environment.

5.1.6.7 Dealing with media.

5.1.6.8 Obtaining emergency services/supplies.

5.1.6.9 Providing security.

5.1.6.10 Providing personnel needs.

5.1.7 Activation of Recovery Procedures:[7]

5.1.7.1 Obtaining authorization to access damaged facilities or geographic areas or both.

5.1.7.2 Notifying personnel.

5.1.7.3 Notifying utilities and other agencies required for resuming business.

5.1.7.4 Obtaining supplies needed for business.

5.1.7.5 Obtaining and installing necessary hardware components.

5.1.7.6 Obtaining and loading backup media.

[6] The U.S. National Archives & Records Administration. www.archives.gov. Vital Records and Records Disaster Mitigation and Recovery: An Instructional Guide.

[7] National Institute of Standards and Technology, Contingency Planning Guide for Information Technology Systems.

5.1.7.7 Restoring critical operating system and application software.

5.1.7.8 Restoring system data.

5.1.7.9 Testing system functionality including security controls.

5.1.7.10 Connecting system to network or other external systems.

5.1.7.11 Resume equipment operations.

5.1.8 Termination of Disaster Recovery Operations:

5.1.8.1 Designated authority declares the end of disaster recovery operations and disseminates that announcement to the communications network.

5.1.8.2 Arrange for all personnel to return to work.

5.1.8.3 Resume standard operating procedures.

5.1.8.4 Complete comprehensive post event evaluation, conduct review of the adequacy of the existing disaster recovery plan, and revise the plan if necessary.

5.1.9 Appendices:[8]

5.1.9.1 Personnel contact information.

5.1.9.2 Vendor contact information.

5.1.9.3 Equipment and system requirements for all hardware, software, firmware, and other resources required to support system operations. Details should be provided for each entry, including model or version number, specifications, and quantity.

5.1.9.4 Key business records.

5.1.9.5 Directions to and description of any alternate sites including locations for offsite backup media.

5.1.9.6 Other documents or information critical to the organization.

5.2 Writing the Plan:

5.2.1 Assign an individual (in case of small organizations) position/department or a team to create the plan. Particular attention should be paid to the coordination of needed input from various departments. When the team approach is used, team members should be individuals who serve in a variety of organizational roles in order to assure a diversity of perspective when creating the plan. Be sure to include the following items within the plan:

5.2.1.1 Designation of the individual position/department responsible for maintaining the plan.

5.2.1.2 Designation of the individual position/department responsible for declaring an emergency and activating the plan.

5.2.1.3 Designation of the individual position/department in charge of making short-term emergency decisions.

5.2.1.4 Designation of the individual position/department in charge of transitioning from emergency mode back to normal business mode.[5]

5.2.2 The essence of writing a disaster recovery plan is to think ahead and create a unified plan that addresses all defined disaster scenarios (internal and external). Be aware that during a disaster, individuals may not be able to call in, log in, or walk in.

5.2.2.1 Natural—hurricane, tornado, flood, snow, ice, fire, earthquake, etc.

5.2.2.2 Human—disastrous employee error, sabotage, virus, terrorism, etc.

5.2.2.3 Environment—disastrous equipment failure, software corruption, telecommunications network outage, electrical failure, etc.

5.3 The Planning Process:

5.3.1 To be successful, senior management must support the plan and be included in the process to develop the policy statement and the plan.

5.3.2 When policies and procedures are developed related to the disaster recovery plan, they need to be coordinated with related organizational activities, including information technology security, physical security, human resources, risk management, quality assurance, information technology operations, and administrative services.

5.4 The disaster planning process should include the following key steps:[9]

5.4.1 Identify and assign responsibility (committee, task forces, or teams).

5.4.1.1 Planning.

5.4.1.2 Response.

5.4.1.3 Recovery.

5.4.2 Train members of the committees, task forces, or teams.

5.4.3 Conduct a risk analysis.

5.4.3.1 Identify potential building problems.

5.4.3.2 Survey fire protection policies and equipment.

5.4.3.3 Assess ability to protect people.

5.4.3.4 Evaluate potential source for damage.

5.4.4 Establish goals and a timeline.

5.4.5 Develop a reporting schedule.

5.4.6 Evaluate systems and records and establish priorities.

5.4.7 Develop recovery strategies.

5.4.8 Identify preventive controls and protection needs.

5.4.9 Review fiscal implications.

5.4.10 Prepare the plan.

5.4.11 Distribute the plan.

5.4.11.1 Training.

5.4.11.2 Testing.

5.4.11.3 Drills/Exercises.

5.4.12 Plan maintenance.

5.4.12.1 Evaluate the plan.

5.4.12.2 Update it regularly.

5.4.12.3 Continue to follow the 3 planning principles of define, document, and demonstrate.[10]

5.5 Plan Characteristics:

5.5.1 Recognizing that the logic and order of recovery steps depends on the nature of the organization and its services as well as on the type of disaster or interruption, the plan should have the following characteristics:

5.5.1.1 Significant flexibility so that the plan can be utilized as needed by managers.

[8] Ibid.

[9] The U.S. National Archives & Records Administration. Vital Records and Records Disaster Mitigation and Recovery: An Instructional Guide.

[10] HIPAA in Practice, The Health Information Manager's Perspective. Available from American Health Information Management Association, Chicago, IL.

5.5.1.2 Able to be implemented without the direct input of the person or the team that created it.

5.5.1.3 Legible, easy to understand, and able to be interpreted by all involved.

5.6 Environmental Assessment and Analysis of Organization:

5.6.1 Determine and list the functions and services provided by the organization.

5.6.1.1 Dictation services for authors or accessing of voice files from client voice servers or both.

5.6.1.2 Delivery of voice files to medical transcriptionists.

5.6.1.3 Processing of transcribed reports.

5.6.1.4 Document distribution to clients or providers or both.

5.6.1.5 Billing or accounting for services rendered.

5.6.1.6 Payroll.

5.6.1.7 Pay for vendor services.

5.6.2 Identify the location of key records, equipment, and supplies that would be needed during a recovery process.

5.6.2.1 Computer(s).

5.6.2.2 File cabinet(s).

5.6.2.3 Onsite location(s).

5.6.2.4 Offsite location(s).

5.6.2.5 Documentation of equipment location both at your site and off-site at your clients, MT homes, etc.

5.6.3 Detail what important information would be needed during a recovery process and prioritize each.

5.6.3.1 Current protected health information to include voice and text data.

5.6.3.2 Stored protected health information to include voice and text data.

5.6.3.3 Business data to include contracts, leases, deeds, service agreements, insurance policies, corporate bylaws, IRS information, banking and accounting materials.

5.6.3.4 The organization's intellectual capital, i.e., the programmer's code for a particular software application.

5.6.3.5 Software/hardware (backups).

5.6.3.6 User names and passwords (limited access).

5.6.3.7 List of all authorized personnel with level of access allowed.

5.6.4 Include details on how this information is stored in a secure environment.

5.6.4.1 CDs.

5.6.4.2 Archived files within digital systems.

5.6.4.3 External drives.

5.6.4.4 Backup media.

5.6.4.5 Intranet.

5.6.4.6 Other.

5.6.5 Have a backup plan for accessing key information during an emergency or system outage.

5.6.5.1 Alternative methods for access.

5.6.5.2 Alternative individuals given access privileges.

5.6.6 Inventory and document all equipment, software, and fixtures (whether recovery-related or not).

5.6.6.1 Consider photo documentation or video recordings with narratives or both.

5.6.6.2 Original invoices for equipment and components with date of installation.

5.6.6.3 Establish an equipment database.

5.6.6.4 Original software with appropriate license agreements.

5.6.6.5 Store a backup of this information in a secure offsite location.

5.7 Communication:

5.7.1 List routine modes and lines of communication both within and outside the organization.

5.7.1.1 Telephone with extension number.

5.7.1.2 Email or Instant Messaging addresses or both.

5.7.1.3 Wireless communication devices.

5.7.1.4 Web-based communication devices.

5.7.1.5 Name and title of individuals involved in routine communication.

5.7.1.6 Other.

5.7.2 When a disruption impacts business operations, communication becomes especially critical. Identifying stakeholders in advance and predefining communication methods can save a great deal of time and effort when a disruption occurs. Consider these examples of a broad range of stakeholders with whom rapid communication might be required.

5.7.2.1 Members of the workforce (employees, independent contractors, students, volunteers, etc.).

5.7.2.2 Board of Directors and/or business owner(s).

5.7.2.3 Customers/clients/healthcare staff.

5.7.2.4 Vendors for customers/clients.

5.7.2.5 Suppliers/vendors.

5.7.2.6 Press.

5.7.2.7 Neighboring businesses.

5.7.2.8 Utilities (electricity, water, trash, sewage, etc.).

5.7.2.9 Telecommunication services.

5.7.2.10 Community emergency services (police, fire, ambulance, civil defense, building inspector, Red Cross).

5.7.2.11 Insurance representatives.

5.7.2.12 Maintenance services (plumbers, electrician, building contractor, etc.).

5.7.3 In disastrous situations, prompt and clear communication with clients/customers or healthcare providers or both can minimize anxiety and panic. Communicate with them immediately. This contact list should include the following items:

5.7.3.1 Product or service provided to them.

(1) Location and description of any remote equipment on their premises.

5.7.3.2 Customer's name.

5.7.3.3 Mailing address (including zip code).

5.7.3.4 Contact person's full name.

5.7.3.5 Contact phone numbers with area code.

5.7.3.6 Email address(es).

5.7.3.7 Instant message provider and address.

5.7.3.8 Alternate names and numbers for emergency contacts.

5.7.3.9 Fax number.

5.7.3.10 Notes or comments (other pertinent information).

5.7.4 Follow a similar procedure for informing vendors of an emergency. Vendor contact list should include the following items.

5.7.4.1 Product or service provided.

(1) Location and description of any remote equipment on the premises.

5.7.4.2 Name of the vendor.

5.7.4.3 Mailing address (including zip code).

5.7.4.4 Contact person's full name.

5.7.4.5 Contact phone numbers with area code.

5.7.4.6 Email address(es).

5.7.4.7 Instant message provider and address.

5.7.4.8 Alternate names and numbers for emergency contacts.

5.7.4.9 A 24-hour phone number.

5.7.4.10 Fax number.

5.7.4.11 Notes or comments (other pertinent information).

5.7.5 Communication with members of the workforce (employees, independent contractors, students, volunteers, etc.). An emergency call list should be kept current to include the following information:

5.7.5.1 Full name.

5.7.5.2 Title.

5.7.5.3 Mailing address (including zip code).

5.7.5.4 Telephone number(s) with area code (including office, home, cellular, or pager, or combinations thereof).

5.7.5.5 Email address(es).

5.7.5.6 Instant message provider and address.

5.7.5.7 Alternate contact information (family, friends, etc.).

5.7.6 Establish an Alert Team composed of key individuals.

5.7.6.1 Declaration of an emergency will be done by designated individual position/department.

(1) Immediately following the declaration of an emergency, the remainder of the Alert Team will be contacted.

5.7.6.2 Determine what information is essential to immediately communicate and who will do it. This will include the primary communication method and an alternative method during the current emergency.

5.7.6.3 Define an order of contact or hierarchy of notification.

(1) Groups to contact include: Members of the Alert Team, remainder of the workforce, clients and healthcare providers, vendors and suppliers, media, and others when the disaster plan has been implemented, when the emergency has been resolved, and when the status has transitioned to a normal business mode.

(2) Determine best method of communication (i.e., phone tree, blast alert system, etc.).

5.8 Incorporate within the plan the appropriate actions for a variety of disaster situations.

5.8.1 Answer the following questions to help design/create the plan.

5.8.1.1 Is this disaster internal to the facility or external?

5.8.1.2 What is the disaster—fire, explosion, bomb threat, tornado, hurricane, snow, ice, water, major power and communication outage, etc.—and what are the responses for each?

5.8.1.3 Here are some examples of disaster situations to use as a guide:

Situation	Action
Disaster inside the building(s) such as a fire, explosion, or other damage to the facility or persons therein.	Call 9-1-1. Relocate staff/patients from the affected areas. Assist those in co-located building if needed.
Disaster in the community/county caused by explosions, wrecks, fires, floods, storms.	Evaluate with community/county emergency services what response would be required by staff.
Disaster threatening the facility or community/county such as identified above.	Implement appropriate disaster plan when situation has been confirmed. Precautionary transfer of staff/patients from the affected areas.
Disaster outside the community/county/state.	Contact workforce or clients or both in affected area to offer assistance.

5.9 *Contingency Planning*—In order to make alternative plans, specifically consider each of the organization's services. If a phone system is needed to provide services to clients or providers, this may be the area that should be invested in redundancy by having phone service with multiple providers. If it is a computer system or a website that is needed to provide services to clients or providers, this may be where to focus resources for redundancy.

5.9.1 Plan for an alternative place for staff to go should the corporate offices or their home offices become unusable; consider remote access for critical applications.

5.9.2 Here is an example of contingency planning for alternative office space:

Facility	Capacity Each Shift	Estimate Minimum Staff	Supplies/Equipment Needed
ABC	4 spaces	1 clerical 3 MT	Employee identification, keys or private access code, phone, internet, computer, printer, backup drives, fax, etc.
XYZ	6 spaces	1 clerical 5 MT	Employee identification, keys or private access code, phone, internet, computer, printer, backup drives, fax, etc.

5.9.3 Establish a contingency plan for the following important items:

5.9.3.1 Privacy and security of individually protected health information, voice and text, digital and paper.

5.9.3.2 Ongoing transcription being performed by remote staff not affected by the disaster.

5.9.3.3 Provision of needed transcription support services.

(1) Evaluation of needs for remote or onsite medical transcriptionists and other staff.

5.9.3.4 Preservation of data integrity.

5.9.3.5 Quality assurance for ongoing transcription.

(1) Evaluation of needs for remote or onsite quality assurance editors.

5.9.3.6 Turn-around time for transcribed documents.

5.9.3.7 Dictation services for authors.

5.9.3.8 Dictation (voice file) access support for medical transcriptionists or clients or both.

5.9.3.9 Transmission or transportation or both of confidential healthcare documentation (paper or electronic or both) to all involved parties.

5.9.3.10 Procedures for handling any material that has been damaged and needs to be recovered or restored, i.e., wet documents, wet or burned hard drives, etc.

5.9.3.11 Procedure to reset passwords in case of system failure.

5.9.3.12 Security services for personnel and facility protection.

6. Organization of Key Business Information and Documents

6.1 Know where the organization's information is so that if staff is displaced from the office, steps can be taken to resume business operations. See Table 1.

6.2 *Personnel Information*—List all names, home addresses, phone numbers, email addresses, emergency contacts, etc. (see 5.7.5 for more details).

	Onsite & where	Offsite & where
I-9s	☐ _____	☐ _____
Payroll		
Company Name		
Account Number		
Payroll Rep		
Phone & email		

6.3 *Insurance Information:*

6.3.1 General Liability/Commercial Umbrella

Company / Underwriter:
Policy Number:
Representative, phone and email:
Broker, phone and email:

6.3.2 Corporate Automobile

Company / Underwriter:
Policy Number:
Representative, phone and email:
Broker, phone and email:

6.3.3 Professional Liability

TABLE 1 Organization Information[A]

	Onsite & where	Offsite & where	Online & url
IRS Determination Letter	☐ _____	☐ _____	☐ _____
IRS Form 1023	☐ _____	☐ _____	☐ _____
Current/previous Form 990s	☐ _____	☐ _____	☐ _____
Current and previous audited financial statements	☐ _____	☐ _____	☐ _____
Financial Statements (if not part of the computer system and regularly backed-up)	☐ _____	☐ _____	
Sales-Tax Exemption Certificate	☐ _____	☐ _____	
EIN #: _____			
ER #: _____			
Bylaws	☐ _____	☐ _____	☐ _____
Mission Statement	☐ _____	☐ _____	☐ _____
Board Minutes	☐ _____	☐ _____	☐ _____
Corporate Seal	☐ _____		
Blank Checks	☐ _____		
Computer Passwords	☐ _____	☐ _____	☐ _____
Client Records	☐ _____	☐ _____	☐ _____
Vendor Records	☐ _____	☐ _____	☐ _____

[A] If a disaster recovery service vendor is under contract, provide contact information in this section.

Company / Underwriter:
Policy Number:
Representative, phone and email:
Broker, phone and email:

6.3.4 Directors & Officers Liability

Company / Underwriter:
Policy Number:
Representative, phone and email:
Broker, phone and email:

6.3.5 Health Insurance Company

Company / Underwriter:
Policy Number:
Representative, phone and email:
Broker, phone and email:

6.3.6 Unemployment Insurance

Company / Underwriter:
Policy Number:
Representative, phone and email:
Broker, phone and email:

6.3.7 Workers' Compensation

Company / Underwriter:
Policy Number:
Representative, phone and email:
Broker, phone and email:

6.3.8 Disability Insurance (short-term)

Company / Underwriter:
Policy Number:
Representative, phone and email:
Broker, phone and email:

6.3.9 Disability Insurance (long-term)

Company / Underwriter:
Policy Number:
Representative, phone and email:
Broker, phone and email:

6.3.10 Life Insurance

Company / Underwriter:
Policy Number:
Representative, phone and email:
Broker, phone and email:

6.3.11 Dental

Company / Underwriter:
Policy Number:
Representative, phone and email:
Broker, phone and email:

6.3.12 Long Term Care

Company / Underwriter:
Policy Number:
Representative, phone and email:
Broker, phone and email:

6.3.13 Retirement Plan/401k

Company / Underwriter:
Policy Number:
Representative, phone and email:
Broker, phone and email:

6.3.14 Other Insurance

Company / Underwriter:
Policy Number:
Representative, phone and email:
Broker, phone and email:

6.4 *Financial Information:*

6.4.1 Financial accounts.

Bank Name(s):
Account Numbers:
Branch Representative:
Phone, fax, email:

6.4.1.1 List those who are authorized to make transfers.

6.4.1.2 List those who are authorized check signers.

6.4.2 Investment

Financial Planner / Broker Company:
Rep name:
Phone, email:

6.4.2.1 List those who are authorized to make transfers.

6.4.2.2 List those who are authorized signers.

6.5 *Technology Resources:*

6.5.1 Since computers are integral to the organization's mission or operations, take the following steps to prepare for resuming information technology functions.

6.5.2 *Inventory—Hardware:*

6.5.2.1 Create a document that lists every piece of hardware that the organization owns and would need to replace if damaged or destroyed. Include the make and model, as well as the serial number, and date installed.

6.5.2.2 Document all printers and other peripherals (scanner, external drives, etc.).

6.5.2.3 Maintain a file containing all the purchase receipts with details of the hardware including date of installation.

6.5.2.4 Document all other technology equipment, i.e., phones, faxes, pagers, beepers, cell phones, etc.

6.5.3 *Inventory—Software:*

6.5.3.1 Document the software version and license number being used on each individual computer and server.

6.5.4 *Network*—Create a diagram of the network structure and workflow.

6.5.4.1 Document the current computer configuration so that backup tapes can be used to restore applications and systems.

6.5.4.2 Map the workflow through the network with security methods utilized (i.e. intrusion-detection devices, encrypted, password protected, etc.).

6.5.5 Maintain a list of technology vendors and contact information.

6.5.5.1 Company that provides website hosting.

6.5.5.2 Company that provides email services.

6.5.5.3 Company that provides telecommunication services.

6.5.6 Document all passwords needed to access files and data and store offsite.

6.5.6.1 List authorized individuals who can reset default system passwords.

6.5.7 Ensure that key individuals know how to program phones to forward to another number, change voice mail messages, retrieve voice mail remotely, reset mail box passwords, and any other necessary features.

6.5.8 *Website*—Ensure that website can be updated from a remote location (outside of the office).

6.5.9 All employees should know how to access their email from alternative sites.

6.5.9.1 Have employees establish backup email accounts for emergency use.

6.6 *Data Integrity*—Analyze the data backup routine.

6.6.1 Create backups, verify the data, and take it off-site. This can be as simple as having someone regularly taking the

backup home to secure in a fire-proof lock-box or it could be high-level, clustering or mirroring the server to ensure data security.

6.6.2 Do a backup, test for validity, and restore.

6.6.2.1 Setup a routine schedule for backups and testing of the backup and recovery strategies.

6.6.2.2 Backups should include all important and pertinent files.

6.6.3 Determine what kind of archival system of the backup media will be maintained.

6.6.3.1 Establish a rotation system for backup media to get to achieve an archive of data.

6.6.3.2 Keep a copy off-site as a theft or loss of the only existing backup tape due to a disaster will not help with data restoration.

6.6.4 Consider making the databases web-based. For example, use an ASP (application service provider) to store the database online.

6.6.5 Consider a redundant data center where information would be mirrored in separate locations.

6.7 *Data Security*—Use technical and physical security measures to protect the data.

6.7.1 Encrypt data and provide a key only to those authorized to view it.

6.7.2 Store media in a fire-proof lock-box.

6.7.3 Use password protection to gain access to systems where data is located.

7. Tips for Mitigating the Effects or Risks or Both of Disasters and Emergencies

7.1 An uninterrupted power supply (UPS), also known as a battery backup system, will supply a limited amount of power in the event of an electrical outage. In the event of power loss, the UPS will allow enough time to shut down the network without causing damage to the server or the data. Periodically test your UPS system to assure the batteries are operational.

7.1.1 Consider replacing desktop systems with laptops where possible because laptops with built-in battery backup may allow users to continue working when power failure occurs.[11]

7.2 Firewalls are imperative for network systems that are online. Firewalls protect data and computing resources, limit access for users, and provide a security and surveillance system for the network.

7.3 Enforce virus scans and updates with network users.[12]

7.3.1 Establish policy to limit user activities to minimal risk of a virus.

7.4 Backup generator systems are now commonly used in businesses and in homes. These generators allow limited electricity usage during an emergency outage.

7.5 Redundancy of systems will allow excellent preparedness for a disaster. Redundancy for electrical, telecommunications, technology, and data may provide an organization with the ability to maintain services even in the face of a current or recent disaster.

7.6 Prepare the office building or premises for emergencies.

7.6.1 Maintain fresh batteries in the emergency lighting system for stairwells and in strategic locations in the building.

7.6.2 Use reflective stair treads with glow-in-the-dark strips to assist in exiting in darkness.

7.6.3 Assure that the fire extinguishers are easily accessible and ample in number. Train all personnel how to use them.

7.6.4 Test emergency exit routes. These should be posted on the back of the restroom doors.

7.6.5 Do routine testing of the fire and smoke alarm systems to assure they are properly working.

7.6.6 Have flashlights with fresh batteries available in strategic locations for use by office personnel.

7.6.7 Maintain a first-aid kit on the premises.

8. Keep the Plan Current

8.1 Once the plan has been developed it is critical to keep it current and available to all key personnel.

8.2 The plan should be reviewed for accuracy and completeness at least annually or whenever significant changes occur to any element of the plan. The review should ensure new information is documented and revised if required.

8.3 Perform analysis of disaster recovery plan and its effectiveness immediately after its use in a disaster or mock disaster drill.

8.4 Archive copies of previous disaster plans.

9. Keywords

9.1 confidentiality; contingency plan; dictation; disaster; individually identifiable health information; medical transcription; recovery plan; security

[11] Disasters Come in All Sizes, Stremple and Martone, March 2000. InfoPro. www.arma.org.

[12] Ibid.