American Health Information Management Association

DISASTER PLANNING AND RECOVERY

TOOLKIT

AHIMA
American Health Information Management Association®

DISASTER PLANNING AND RECOVERY

TOOLKIT

ISBN: 9781584265634
AHIMA Product No.: ONB202016
AHIMA Staff:
Chelsea Brotherton, *Assistant Editor*
Jewelle Hicks, *Publications Manager*
Pamela Woolf, *Director of Publications, AHIMA Press*
Anne Zender, *Senior Director, Periodicals*

For more information about AHIMA Press publications, including updates, visit ahima.org/publications/updates.aspx

American Health Information Management Association
233 N. Michigan Ave., 21st Fl.
Chicago, IL 60601

AHIMA.ORG

TABLE OF CONTENTS

Foreword 4
Authors and Acknowledgements 5
Introduction 6
Types of Disasters 6
Planning 6
- Drafting the Business Continuity Plan (BCP) 6
  - Risk Assessment and Analysis 7
  - Downtime and Contingency Planning 8
  - Disaster Recovery Plan 8
  - Data Backup Plan 9
  - Emergency Mode Operations Plan 10
- Education and Training 11
- Practicing and Drills 11
- Planning for Volunteers 12
- Patient Advocacy 12
  - Personal Health Record (PHR) and Patient Portals 12
  - Assisting Patients with Recovering their Health Information 13

Operations 14
- Communication 14
  - Communication Plan 14
  - Identifying Patients 14
  - Releasing Information Involving Victims 15
  - Visitors/Relatives 15
  - Immediate and Short-Term Concerns Checklist 15
- Interim Management 16
  - Staffing: Locating, Communicating with, Caring for, and Managing 16
  - Planning and Continuity of Care 16
  - Emergency Credentialing and EHR Access 17
  - Locating and Discharging Patients 18
- Protecting Health Information 18
  - Paper Record Transfers 18
  - HIPAA and Privacy and Security 18
- Use and Disclosure/Release of Information 18
  - The Joint Commission 19

Recovery 20
- Evaluation, Inventory, and Recovery Plans 20
- Debriefing 21
- Matching and Tracking Tests 22
- Record Preservation 22
- Audit, Control, and Maintenance 22

Appendix A: Sample Contingency Plan 26
Appendix B: Sample Staff Competency List 29
Appendix C: Immediate and Short-Term Concerns Checklist 30
Appendix D: Sample Emergency Privilege Application and Release Form 32

FOREWORD

The Disaster Planning and Recovery Toolkit addresses multiple Information Governance Principles for Healthcare (IGPCH)™. Healthcare entity information assets must be protected to ensure they are secure, reliable, available, and used in an efficient, ethical, lawful, and secure manner even in the face of a disaster. Disruptions, both planned and unplanned, may make electronic health records (EHRs) and other IT assets unavailable to clinicians and other workforce mentor for day-to-day business operations. When planned and accomplished successfully, disaster planning provides several benefits designed to account for the overall recoverability and resiliency of a healthcare organization. The Disaster Planning Tool Kit addresses these requirements with emphasis on data backup plan availability as well as integrity of information.

The IGPHC Principle of Protection requires that healthcare organizations have adequate levels of protection from corruption or loss of information essential to business continuity. The Disaster Planning Toolkit outlines recovery plan components and how to address items including strategies, responsibilities, requirements, and procedures for the processes of recovery.

The toolkit outlines the importance of testing for backups, which is outlined in the IGCH Principle of Integrity as a requirement to ensure reliability, validity, and integrity of systems.

This principle also outlines the expectations by patients, consumers, stakeholders, and other interested parties such as investors and regulatory agencies that the integrity of the information is directly related to the organization's ability to prove that information is authentic, timely, accurate, and complete. The Disaster Planning Toolkit outlines requirements by the Office for Civil Rights (OCR) for steps needed for recovery and reconstruction of data and documentation of the recovery process to outline the integrity.

The Principle of Availability and Principle of Retention outline needs for information to be available and in a manner that ensures timely, accurate, and efficient retrieval throughout its retention period.

Accessibility through currently and readily available access points or devices is applicable to all types of stored information, including, but not limited to, clinical and nonclinical information regardless of storage medium. To mitigate the effects of a disaster, system malfunction, or data corruption, information should be backed up routinely. Regulations such as the HIPAA security rules are not prescriptive in how healthcare entities develop and use disaster recovery and contingency plans; however, there are key points which must be addressed.

Disaster planning is one way healthcare organizations demonstrate maturity and competency in their Information Governance programs. This toolkit assists in this process by providing a sample contingency plan, sample staff competency list, and an outline of useful tips for implementation that is key in the IG Principle of Protection. The tool kit also outlines steps necessary for a data backup plan to address data availability as well as integrity of the information needed by the healthcare organization, and it outlines elements of a functional back up plan and data recovery principles.

By following the Information Governance Principles for Healthcare (IGPCH) in advance of a disaster, organizations are more likely to mitigate and lessen risk to the organization and the patients/individuals that trust in delivery of healthcare.

AUTHORS

Julie A. Dooling, RHIA

Theresa Rihanek, MHA, RHIA, CCS

Diana Warner, MS, RHIA, CHPS, FAHIMA

Lou Ann Wiedemann, MS, RHIA, CDIP, CPEHR, FAHIMA

ACKNOWLEDGEMENTS

Cecelia A. Backman, RHIA, MBA, CPHQ

Barbara Bosler, JD, MPH, RHIA

Alaina Capanna

Tracy A. Clark, MS, RHIA

Kathy Downing, MA, RHIA, CHP, PMP

Kim Turtle Dudgeon, RHIT, CMT

Margaret M. Foley, PhD, RHIA, CCS

Lou Galterio, MBA

Jennifer Gholson, RHIT

Aviva M. Halpert, MA, RHIA, CHPS

Seth Katz, MPH, RHIA

Robyn Kelley, CCA

Beth Liette, MS, RHIA

Cindy C. Parman, CPC, CPC-H, RCC

Lori L. Richter, MA, RHIA, CPHIT, CPEHR, CHPS

Sharon Slivochka, RHIA

Lydia Washington, MS, RHIA, CPHIMS

ORIGINAL AUTHORS

Jill Burrington-Brown, MS, RHIA

Patricia Cunningham, MS, RHIA

Gwen Hughes, RHIA

ORIGINAL ACKNOWLEDGEMENTS

Jill Clark, MBA, RHIA

Angela K. Dinh, MHA, RHIA, CHPS

Aviva M. Halpert, MA, RHIA, CHPS

Beth Hjort, RHIA, CHP

Harry Rhodes, MBA, RHIA, CHP

Mary Stanfill, MBI, RHIA, CCS, CCS-P, FAHIMA

Allison Viola, MBA, RHIA

Diana Warner, MS, RHIA, CHPS

Melva Visher, MA, RHIA

Lou Ann Wiedemann, MS, RHIA, CPEHR

INTRODUCTION

Disaster planning requires healthcare organizations to visualize events that may never happen and often requires imagining mass-casualty situations. In recent years, the United States has seen its share of disasters, ranging from F5 tornados to terrorist bombings. After experiencing these tragedies, imagining a large-scale disaster and mass-casualty event is unfortunately no longer difficult. As a result, disaster planning and preparedness have come to the forefront of HIM and healthcare at large.

Disasters interrupt the essential functions and services of an organization such as patient care, electricity, water, and communications. The interruption can be severe and include the loss of priority services for an extended period of time. Service interruptions can have lasting effects on the organization and community. Well-planned disaster responses will enable patient care and essential functions during and following the event.

TYPES OF DISASTERS

Disaster management is the organization, management, and response for dealing with all aspects of an emergency event. A disaster is any type of sudden natural or man-made event that results in substantial physical damage, loss of life, or a drastic change in the area's environment. There are many types of disasters.

Disasters can be categorized as acts of nature or acts of man.

Acts of nature are considered natural disasters. These include events or occurrences such as earthquake, flood, fire, tornado or hurricane. Another non-weather related act of nature could be an "infectious disease outbreak." This incidence could require organizations to implement disaster protocols and even request external assistance to handle the influx and management of patients. This example may not be immediately recognized at the time of the initial exposure of the infectious agent, so the point of disaster may be difficult to identify.

Acts of man can be broken into two categories; intentional and unintentional.

Examples of intentional acts include theft, civil unrest (rioting and looting), terrorism and computer viruses, worms, hacking, or other malicious code.

Examples of unintentional acts include transportation accidents like a plane crash or a chemical contamination such as toxins being spilled or improperly handled. In addition, "errors and omissions" can cause flooding or fire due to a mechanical failure or faulty system wreaking havoc on both paper and electronic record systems.

PLANNING

DRAFTING THE BUSINESS CONTINUITY PLAN (BCP)

As a means of communication about an individual's health status, health records perform a vital function during disasters. An unexpected loss of an individual's health records could be devastating to the patient, organization, and clinical care providers. Therefore, a well-designed action plan will help organizations resume or maintain operations more efficiently in the event of disaster.

The health record serves a variety of purposes, one of which is to provide an accurate summary of a patient's health status. An unexpected loss of patient health records could be devastating to the patient, organization, and clinical care provider. Therefore, the health record must be guarded against unexpected losses due to a disaster. A well-designed plan with subsequent action plans will help organizations resume business operations more efficiently and effectively after disaster occurs.

Every organization must have a comprehensive plan that protects patient safety, secures health information from loss or damage, ensures stability in continuity of care activities, and provides for orderly and timely recovery of information. This comprehensive plan is often referred to as a business continuity plan (BCP). It is the umbrella that includes separate plans delineating downtime and contingency, disaster recovery, and data backup procedures, all of which are discussed below. The BCP's objectives include protecting human life, maintaining patient services or services to members of a health plan with little or no interruption, lessening the overall impact on an organization, and complying with applicable laws and regulations.

The development of the BCP is an iterative process that needs ongoing attention. It should involve an interdisciplinary team, including a variety of departments and stakeholders, and must be championed and funded by senior management.

Team members must commit adequate time and resources to business continuity planning and training. Areas of involvement should address:

- The relationships with local and community emergency response teams and agencies
- Understanding how responses to the disaster should be born out of planning, drilling, and teamwork inside and outside the organization to include community involvement
- Partnerships with community planners, state hospital associations, and local medical societies

Other considerations and additional information may need to be researched and considered before drafting the BCP for health records and information. Research should be based on organizational type and activities may include:

- Performing a literature search on disasters and disaster planning relative to medical records or health information, including AHIMA's Body of Knowledge at ahima.org, as well as other web pages for additional resources such as the Federal Emergency Management Agency (fema.gov)
- Researching other organization's plans for continuity of health records and information
- Collecting sample health information disaster plans from peer organizations
- Talking to colleagues who have experienced the types of disasters your facility could expect
- Determining to what extent the facility's insurance covers the costs associated with disaster planning such as moving health information, operating elsewhere (including over state lines), recovering damaged information, and lost revenue caused by the inability to restore information. In addition, determine whether your insurer offers consultations and advice about disaster planning. Many insurers provide this at little or no cost to their clients
- Consider video recording your assets for inventory. Viewing assets on video may help to account for and/or trigger memories of what was in a certain area, room, or space

Once necessary requirements and organizational needs are understood, the plan should be drafted. Depending on organizational requirements, structure and need, various elements will make-up organizational policy. The following are separate areas included in a BCP and are covered in some detail below:

- Risk assessment and analysis
- Downtime and contingency planning
- Disaster recovery
- Data backup
- Emergency mode operations

Risk Assessment and Analysis

A risk assessment needs to be conducted prior to creating a comprehensive plan such as the BCP. Risk analysis involves a process of assessing the likelihood that a given threat will occur. It provides direction for planning business continuity and disaster recovery as well as for implementing appropriate security safeguards and controls to prevent and mitigate threats. Risk analysis primarily focuses on applications and the information systems supporting the applications. An assessment of the safeguards governing operational practices such as policies, procedures, responsibilities, and training would also be included in a thorough risk analysis.

The Health Insurance Portability and Accountability Act (HIPAA) and some accrediting agencies include requirements for risk assessments. HIPAA calls for organizations to develop a risk assessment plan to review potential disasters and create a plan to follow when disaster strikes. This applies to covered entities (CEs) and business associates (BAs) alike. In addition, The Joint Commission emergency operations standards require hospitals to describe how staff members will be assigned to cover essential functions during a disaster response.

During the risk assessment and analysis, HIM professionals should work with IT and other stakeholders to ensure key processes and systems that support the electronic health record (EHR) such as document management, computer-assisted coding, release of information, transcription, and billing are assessed and that any identified risks are appropriately addressed.

In addition, considerations must be given to any system that may exist outside the proverbial four walls of the organization such as health information exchanges (HIEs) or other third-party vendors that receive or share PHI.

Given the criticality of correct patient identification during a disaster, the risk analysis should also focus on critical systems such as the master patient index (MPI). Other risk analyses would focus on operational and organizational practices like policies, procedures, responsibilities, staffing, training, off-site storage of records or backup media, and archiving records.

The US Department of Commerce, National Institute of Standards and Technology (NIST–updated September 2012) Special Publication 800-30—Guide for Conducting Risk Assessments, Information Security, is a comprehensive resource that outlines the fundamentals of a risk assessment as well as preparing for and conducting a risk assessment.[1]

Downtime and Contingency Planning

The downtime plan focuses on sustaining business functions during short interruptions that would not be classified as a disaster. These events would include an unintentional man-made disaster such as an internal flood due to facility construction. For organizations primarily using EHRs, downtime procedures usually require switching to another form of documentation capture such as a paper-based system.

For contingency planning, whether it is an unintentional manmade disaster or an intentional manmade or natural disaster, make a list of the various types of disasters (location and facility specific) that might directly impair the operation of the facility, such as fire, explosion, tornado, hurricane, flood, earthquake, severe storm, bioterrorism, or extended power failure.

Next, list your department's core processes. For example, this may include maintenance of an accurate MPI, coding, document management and imaging, release of information, revenue cycle, transcription, and EHR documentation and reporting. For each plausible disaster and core process, generate a contingency plan. (See Appendix A, "Sample Contingency Plan.")

The HIPAA security rule applies to electronic PHI only; however, in order to comply with the privacy rule, back-up and recovery of all PHI must be provided for, regardless of its origin or medium. The HIPAA security rule requires procedures for restoring data, responding to a disaster that damages systems containing electronic PHI, recreating copies of destroyed electronic PHI, and functioning in emergency mode.[2]

For more information on 10 security domains that provide a foundation of security principles and practices, refer to AHIMA's "10 Security Domains" practice brief in the AHIMA Body of Knowledge. (Note: These domains are different from the HIPAA security rule.)

Disaster Recovery Plan

This plan refers to a major, usually catastrophic event that leads to downtime for an extended period of time. What sets this plan apart is that it describes the process and thresholds for declaring a disaster. To ensure organizational consistency, the information technology (IT) disaster management plan should be inextricably linked to the institution's overall disaster plan.

The plan should lay out the criteria that will determine how crucial decisions will be reached. For example, in an emergency department scenario:

- Should visits be back-loaded into the master patient index?
- Should orders be integrated into existing records, regardless of whether they are in paper or electronic format?
- If emergency records are not integrated into existing records, should they be interfiled or stored separately?

The plan should also account for the security of the premises, since the greater the disaster, the less likely the perimeter of the premises will be secured and the greater the risk that PHI will be accessed inappropriately. Plans for physical security of PHI should be developed in advance for various degrees of disaster, including designating or preparing metal cabinets if paper records are used, preparing schemas for maintaining staffing rosters, creating a process for work schedules, and issuing temporary ID badges for volunteers and other first responders who will need access.

Data Backup Plan

The data backup plan addresses data availability as well as integrity and is a critical element in protecting health information. Each application and information system should have a formal, documented data backup plan. Frequency of backups and backup testing should be included in the plan as well. A disaster plan must comprise both a mechanism for backing up data before disaster hits and for recreating it after systems crash. The plan must also provide a procedure for documenting concurrent clinical findings during the disaster in a manner that will be retrievable after the disaster recedes.

If a hot site or high-availability system is available, the system should "fail over" automatically to ensure continuity of care. The actual backup of all the elements outlined in the plan should be implemented as soon as feasible. In all likelihood, a variety of smaller back-up plans and processes are already in place. All existing plans and processes should be surveyed, evaluated for compliance, and either included in the plan or replaced with a compliant version. No backup process should be discontinued until a replacement process is available for immediate implementation.

Physical security is vital at the backup site and during the recovery process. Access to data backed up off-site should be subject to the same protective controls as access to on-site data. Only authorized personnel should have access to such backups during the storage process and any subsequent retrieval and recreation of lost data. All access should be tracked and monitored. Data carefully backed up on media not protected from theft, flood, fire, or other risk will be no more available if a disaster hits than data not backed up at all.

A functional backup plan must go further than just the HIPAA privacy and security rules. It should include:

- Processes for backing up all data on all systems, as well as steps for recreating all components of the health information system
- Description and location of all components of the electronic, hybrid, or paper records, and the configuration of any networked device including hardware and software deployed
- Processes for recreating data tables, contracts, licenses, and policies and procedures
- Assignment of responsibility for each component which identifies backup personnel if key individuals are inaccessible or incapacitated
- An estimate of how long the organization or provider can continue to function at various stages of recovery

Data recovery is the part of the process least affected by the privacy rule. It is important to remember, however, that to provide future patient access to health records, enabling the right to amend a record or to respond to authorization to use and disclose PHI; the PHI must be restored in a usable format in a relatively quick and efficient manner. Standard data recovery principles should be applied during the planning and back up periods, including:

- Provisions for reading data that were created on applications that may no longer exist by transforming the data into a human readable format prior to "sunsetting" a system
- Implementing data retention policies that include predetermined data destruction timetables
- Maintaining the currency of the backed up versions of policies and procedures for recreating the network environment, as outlined above
- Developing a realistic estimate of how long the institution can go without preexisting data and creating an interim plan that realistically matches the anticipated recovery timetable

Once the disaster itself has subsided, the recovery plan must take into account the eventual need to comply with patients' rights. This includes the right to access their entire medical records or designated record sets, amend their records, and receive an accounting of disclosures.

Documentation will be critical for billing, providing birth and death certificates, and enabling necessary legal activities.

The obstacles to achieving these goals during the disaster could include challenges in:

- The documentation process
- The physical environment
- Communication
- Untrained volunteers

The long-term impact of these obstacles may include skimpy documentation and scattered chart components, which in turn will likely result in problems with future retrieval efforts.

Despite the most carefully laid plan, disasters by their nature include circumstances that cannot be anticipated. Although a well-designed plan will anticipate many decision points, it will not be possible to anticipate all of them. A BCP should, however, provide a procedure for making decisions under pressure.

Emergency Mode Operations Plan

The emergency mode operations plan can also be referred to as a crisis management plan. This is the plan that starts with the declaration of the disaster and continues until the organization fully returns to its pre-disaster operational status. Some processes described in this plan are workflows, physical security, emergency purchases, access controls, configuration management and change controls, reports, supplies, and inventory control. Other processes may be added after a practice drill reveals necessity.

A standardized emergency mode may include elements such as:

- A communication plan defining the scope of the outage to staff, the extent of resources disabled, and the extent of recovery and restoration as it occurs
- Minimal documentation requirements
- Emergency registration sets that can double as a source of patient identification mid-crisis and, ultimately, a means of filing the patient's PHI
- An emergency paper chart that enables and expedites the standards agreed upon
- Downtime procedures for paper documentation
- Stickers for allergies and other emergency flags
- Standardized filing procedures based on a predetermined manual numbering system that can be accessed at a later date to retrieve emergency mode documentation

Note: The Pandemic and All-Hazards Preparedness Reauthorization Act of 2013 was updated from the original legislation in 2006 when Hurricane Katrina revealed weaknesses in responses and coordinated efforts. Following more recent disasters such as the Joplin tornado in 2011 and Superstorm Sandy in 2012, the act provides more flexibility for state health departments and how they use staff during a disaster. The act also gives greater authority to the Food and Drug Administration to authorize the emergency use of certain products as medical countermeasures.[3]

EDUCATION AND TRAINING

Part of the BCP should include formation of internal incident response teams within the organization. Training must be ongoing throughout the year to keep skills and expertise up-to-date. Examples of the types of incident response teams can include privacy, information security, and legal/compliance.

Practicing and Drills

A plan is only as strong as the people who execute it. A documented, finalized, and approved disaster recovery plan must be implemented, tested, and reviewed by all staff to ensure its overall compliance and success. In addition to training, performing test runs of the plan is imperative in identifying gaps and any needed enhancements or changes.

Listed below are some useful tips for implementation:

- Perform the preparatory activities listed in each of the contingency plans (examples of these activities are listed in Appendix A, "Sample Contingency Plan").
- Share the preliminary plans with the appropriate organizational committee.
- Provide staff with the training and tools necessary to implement the plan. (See Appendix B, "Sample Staff Competency List.)
- Test the plan. Retest the plan.
- Drill until the plan fails. Evaluation and critiquing drills will improve the plan.
- Re-evaluate and revise the plan and corresponding procedures based on the results of testing and simulated disaster trials. Input should be collected from all staff, including the safety officer, risk manager, and privacy and security officials.
- Include disaster training as part of staff orientation.
- Measure staff competency by asking staff to describe or demonstrate their roles and responsibilities during specific disasters.
- Include competencies in staff performance standards on an annual basis.
- Establish a plan for:
    - Conducting drills (announced and unannounced)
    - Reviewing and updating the plan
    - Staff training and review
    - Planning execution and enforcement

Remember that although orderly drills are helpful, the disaster itself will not be orderly:

- Control as much as possible ahead of time.
- Plan for more disaster victims than the organization will likely ever receive.
- Plan that victims will arrive at all hospital entrances and expect that collecting information will not be easy.
- Traditional admitting and discharge procedures will be impossible.
- Your facility should have a patient identification system that is simple and ready for use, enables tracking of the patients later by investigative authorities, and allows for the finding of the patients by relatives. (For more information on identifying patients, see the section "Communication–Identifying Patients" below.)

Planning for Volunteers

People will come to the facility to volunteer during a disaster, and unless the facility is prepared for them, they can hinder operations. The organization should decide in advance if the use of nonemployees will occur and if so, designate a volunteer coordinator. Make plans for those who can help with administrative functions and volunteer clinicians who can treat patients. Further, determine if and how credentials of healthcare practitioners will be checked. Have adhesive-backed name badges on hand to identify approved volunteers at a glance. The organization must decide if there are roles for volunteers from the community and if they should be certified in emergency planning such as Federal Emergency Management Agency training.

See "Emergency Credentialing and EHR Access" in the "Operations–Interim Management" section on page 16 for more information on communication and credentialing professional practitioner volunteers.

PATIENT ADVOCACY

Personal Health Record (PHR) and Patient Portals

Many healthcare providers are implementing portals in conjunction with their EHR to allow patients access to their health information. Such portals can aid consumers during a disaster since they offer secure, online, and remote access to selected health information such as the names of health care professionals, medications, allergies, and other information that could prove critical during a disaster planning since they offer secure, online, and remote access to selected health information.

However, even with this technology consumers must be educated on preparing for a disaster without the use of technology. One suggestion is to encourage consumers to carry a list of medications they and their family members take on a daily basis. This list should include dosages, any allergies, and other pertinent and special needs such as serial numbers on medical devices. It should also contain contact information of providers, close friends, and family. The list can be created on a small card to carry in a wallet.

In either case, patients should be educated on the importance of accessing portal information online and creating and about maintaining their personal health information.

For more information on PHRs, patient portals, and the consumer's role, visit myphr.com as well as AHIMA's Body of Knowledge (BoK) at ahima.org.

Assisting Patients with Recovering their Health Information

Originally published by AHIMA in the aftermath of Hurricane Katrina, the revised list below may be used to assist patients with recovering their health information following a disaster.

When people are displaced by disasters, it can be difficult to begin or resume medical care without healthcare information normally available from a provider's office. For individuals who are attempting to recover their health information, AHIMA suggests the following actions:

- If you have access to the Internet, take advantage of the free resources at myphr.com, a site that offers guidance to understanding and managing one's personal health information.
- If you are active duty military and have a HealtheVet account, explore the VA's Blue Button Initiative to obtain your records: http://www.va.gov/bluebutton/.
- The Centers for Disease Control and Prevention offer the "Keep It With You: Personal Medical Information Form," a voluntary, temporary record that lists medical care and other health information for people who need care during disasters. If you do not have access to the Internet, call your local health department for assistance.
- Call your healthcare providers to see if they are in business or have left contact information. If you can contact them, find out the status of your medical records. Ask them if they have kept backup copies of medical records, lab reports, x-rays, pharmacy, or bills that would be helpful to you.
- Contact your insurance company. It is very likely they can provide documents used in billing (for example, the explanation of benefits statement) to help rebuild your medical record. If you use Medicare, contact the Centers for Medicaid and Medicare Services online or call 1-800-MEDICARE.
- Contact your pharmacy. Many national chains keep records of your prescriptions and can verify names and dosages for you and your healthcare provider, even if you are in a different location.
- Contact your state Department of Health for information contained in Medicaid program information, Women, Infants, and Children (WIC) program information, or registries such as communicable disease, immunizations, and birth certificates. Telephone numbers for state departments of health can be found here through the Centers for Medicare and Medicaid Services (CMS).
- Contact any healthcare providers you have seen on a referral basis (such as home healthcare providers, specialists, surgeons, etc.). They should have information sent to them by your referring healthcare provider.
- If you have children, your school district may be able to provide information from the school nurse about your child. If your child has attended college, contact the college for any health information on file.
- Ask your family to help you remember your medical history as you write it down.

OPERATIONS

COMMUNICATION

Communication Plan

Internal and external communication will be complicated and communication planning is critical.

Organizations should develop:

- A communication team with plans for each member, including the CEO
- An off-site, alternative location for a disaster control center response unit
- Backup communications in case normal systems are down:
  - Internal communications might include messenger systems and radio systems such as two-way and ham as well as cell phone systems. They might also include use of e-mail.
  - Staff communications regarding expected admissions, arrival times, and frequent updates must be addressed. Also, incorporate the ability for staff to communicate with their own families during the crisis.
  - External communications should include developing relationships with telephone and communication companies able to bring in mobile equipment.
  - Communication procedures should be shared among area treatment facilities to consolidate the location of disaster victims.

Communication will be difficult so checklists can be extremely helpful in times of disaster:

- Maintain an up-to-date list of important contacts and store it in electronic and paper form.
- Keep a copy in your wallet along with personal contacts.
- Categorize staff cell phone numbers by service provider. Past experiences have shown that certain providers' cell towers may not be operational and a list could help to quickly identify those who may or may not have service.
- Include state hospital association contacts, local medical societies, and other pertinent organizations.

Texting or an automated notification system may also be used. Use intranet and social media if the natural environment allows for it.

Planning for media is important to the communication process. The media must have their own space away from treatment areas. The facility should identify a public relations person responsible for communicating with the media who is also linked to the emergency management system (EMS) and communications department.

Identifying Patients

Proper identification of patients and victims may be one of the most difficult operational issues during a disaster. Patient identification during a mass-casualty event must be well planned and executed. Gathering information from the patient and determining a way for this information to remain attached to the patient are the difficult issues. In some situations, the patient may be unresponsive and unable to communicate effectively with care providers. Organizations should clearly define how these patients will be identified for treatment purposes, but also in regards to questions that may arise from outside requestors, e.g., family members looking for someone. See "Use and Disclosure/Release of Information" in the "Protecting Health Information" section below for further guidance on handling these types of requests.

The atmosphere will likely be chaotic, but every patient will need to be identified in some manner. HIM professionals can serve as a resource to their organization in identifying best practices for ways to identify patients and release information during a disaster.

A simple and ready-to-use system for admission and registration is a necessity. Consider the following:

- Pre-numbered tags or other markers that can be attached to the patient/person in multiple ways (clipped or tied).
- Disaster tags should be stored in a secured location from where they may be easily retrieved.
- The use of check boxes on the tag, colored tags, or colored markers to determine gender, hair color, race, eye color, and age (child, adolescent, adult).
- Descriptions like "gray-haired female, blue dress, black shoes" may help to later identify the patient.
- A consistent process to identify unknown patients (unable to speak, comatose, etc.) must be in place.
- Patients may have valuables that will need to be collected and tracked. Organizations should determine the best manner of collection and storage of such valuables within their facilities and what personnel should be in charge of this process.
- Location of where the patient arrived. During disaster, there could be many entry points such as "west entrance."
- Consider keeping an inventory of pre-numbered paper charts in multiple locations.

Releasing Information Involving Victims

The rules for release of information are somewhat different in a disaster. HIPAA regulations allow for disclosure of personal health information in a disaster for the purposes of notifying a family member of a patient's location, general condition, or death (Sec.164.510):

4) Uses and disclosures for disaster relief purposes. A covered entity may use or disclose protected health information to a public or private entity authorized by law or by its charter to assist in disaster relief efforts, for the purpose of coordinating with such entities the uses or disclosures permitted by paragraph (b)(1)(ii) of this section. The requirements in paragraphs (b)(2) (b)(3), or (b)(5) of this section apply to such uses and disclosures to the extent that the covered entity, in the exercise of professional judgment, determines that the requirements do not interfere with the ability to respond to the emergency circumstances.
    - So (b)(1)(ii) is that PHI of current care may be released to a friend or family member.
    - (b)(2)(ii) is that the CE does not have any reason to believe the individual would object to sharing PHI as it directly related to the current treatment.
    - (b)(3)If the individual cannot agree or object because of the individual's incapacity or an emergency circumstance, the covered entity may determine to disclose only the PHI that is directly relevant to the person's involvement with the individual's care or payment related to the individual's healthcare or needed for notification purposes.
    - (b)(5) Same as (b)(3), but on deceased individuals.

Verify individual state guidelines covering specific rules regarding access to personal health information in a disaster.

Visitors/Relatives

Visitors and relatives should be located in a designated area apart from the treatment area and the media. A process will need to be in place to inform family members of the patient's location and a communication mechanism to allow them to make inquiries.

The facility should make sure staff members trained in regulatory privacy requirements are in charge of information dissemination. The facility should also have trained professionals who are on call to provide support for counseling, grief, and victim location.

Immediate and Short-Term Concerns Checklist

In the event of disaster, immediate concerns require focus and care of immediate needs and provide short-term solutions: Refer to Appendix C, "Immediate and Short-Term Concerns Checklist" to assist in planning your communication response and take practical steps towards securing your employees, department, and protected health information (PHI).

INTERIM MANAGEMENT

Staffing: Locating, Communicating with, Caring for, and Managing

One of an organization's greatest assets is staff. In the event of disaster, how staff members are located, communicated with, and cared for may be the difference between a successful plan and utter chaos. There are multiple options for locating and communicating with staff.

- Maintain an up-to-date phone or "calling" tree to notify and account for employees.
- "Calling" or phone trees begin with a small group of people and cascade down to all employees.
- When activating the phone tree, employees need to know whether to come to work or stay at home.
- For more information on phone trees, see "Appendix C, Immediate and Short-Term Concerns Checklist."
- In addition to the phone tree, organizations are investing in automated notification systems. These automated systems call or text employees and other predetermined individuals informing them that a disaster event or incident has occurred and whether or not they should report to work or take other action(s).
- If the Internet is available, use e-mail and social media to locate and communicate with employees.
- Ensure badge policies are followed so staff can be easily identified and areas are secured. A central location for staff check-in and check-out should be established to determine who is on the organization's premises.

Plan for and educate staff that their roles will likely be different for some time following a disaster. Staff may be asked to fulfill roles outside their usual daily tasks, such as performing patient advocacy duties or transporting injured patients. It is quite likely that they will be asked to work in tight and confined areas under stressful conditions.

Every employee must know his or her role in a disaster. Departmental plans should be updated and available to employees. Employees should be trained at a minimum at orientation and during annual training. Organizations should also conduct departmental and facility-wide drills and should consider involving the community.

The human resources department should be consulted on personnel policies and communications to staff members. Work and payroll schedules, benefits, and use of vacation time, sick time, FMLA, etc., should be communicated to employees as soon as possible.

Plan for providing such provisions for employees such as being stranded, lockdown, martial law, or environmental barriers that prevent leaving or arriving. Consider safe sleeping areas, scrub distribution, shower and restroom facilities, food and water, and if possible access to phones or mobile device so they can communicate with their families.

Planning and Continuity of Care

Organizations must maintain certain functionality when a disaster occurs, regardless of its severity. The initial challenge during a disaster—whether it is man-made or natural, local or extensive—is to provide continuity of care. In order to do this, organizations must:

- First enable the provision of immediate care
- Next, document the care that was provided and ensure health data are accessible for continuity of care
- Finally, enable access to existing documentation of previous care

Once basic functionality is restored, HIPAA requirements must be addressed with proper planning and care. The aspects of the privacy rule that apply during this interim period include:

- Managing a patient directory
- Controlling use and disclosure of PHI
- Managing business associates within the constraints of a business associate agreement
- Ensuring the physical security of the PHI
- Creating the appropriate documentation that will enable patients to access their designated record set, request amendments, and even produce a rudimentary accounting of disclosures

Emergency Credentialing and EHR Access

Clearly delineating responsibilities in the plan will help reduce confusion when disaster strikes. When Mercy Hospital in Joplin, MO, sustained a direct hit from an F5 tornado in 2011, credentialing information was not readily available. Allison Jungmann, medical staff coordinator for Mercy, advises maintaining a copy of policies and bylaws that refer to disaster or emergency credentialing in all locations. She also warns that the process of verifying a valid license was difficult: "We used the badges they had from other facilities at first to allow them to work if they were not familiar to us. We had a unique situation in that most of our medical staff lost their offices, so we did not have volunteer providers for a period longer than the 72 hours that is required to perform credentialing."

Knowing who is responsible for logging independent practitioners and physicians who volunteer to help will be very important in identifying who documented in the health record. Mercy in Joplin used a whiteboard to schedule shifts. "If you tell them you don't need them, they might not come back," Jungmann says. "If you tell them the time you need them, they will report back when they are needed. This was a huge help for us."

Consider the following questions when developing a plan for approving privileges:

- Who approves and verifies privileges?
- What is the timeline? As soon as the immediate situation is under control (allowing for lack of communication or lack of resources)?
- Who is responsible for providing the access to information systems?
- If paper is used, who is responsible for creating and maintaining the signature identifier log?
- Who is responsible for tracking all volunteers and when and where does this occur?
- Is the process included in the hospital's or organization's bylaws?

For a sample application and release form used to gather information to verify practitioner's current license and competencies to grant emergency privileges, refer to "Appendix D, Emergency Privilege Application and Release Form."

Policies and procedures outlining who will be responsible for not only providers but vendors and contractors who may be on-site at times of disaster are a necessity. Keeping an updated list of eligible providers with premade temporary badges is suggested, since it is likely that electrical components such as printers may not be functioning.

The storage location and retrieval process for the temporary badges will need to be carefully considered in the disaster plan since many environmental factors may inhibit access.

Discussions between facilities should include pre-arrangements to gain access to the facility's EHR during times of disaster. During Superstorm Sandy, physicians were seeing patients in different hospital(s) and utilizing EHRs where they may have had little or no previous training. If hospital A transfers patients to hospital B due to facility damage or overload, providers from hospital A will need guidance and training on how to access and use their EHR while caring for patients at hospital B. This is especially true if the hospitals do not share the same EHR or HIE technology. For this reason, careful community collaboration should be included when creating disaster plans.

Locating and Discharging Patients

Unless there is a formal process in place for discharging patients during a disaster, the organization will not know the disposition or location of patients.

While a discharge process does not initially seem important during a disaster, location and disposition needs to be tracked. Staff especially need the location and disposition to be able to communicate with numerous individuals asking for information during the disaster.

Process considerations may include:

- What kind of system will be used to track this information?
- Is there a preprinted form for the paper process?
- Is there a workaround for reconciling medication lists, documentation of allergies and contraindications, since these are likely captured as "flags" in the EHR?
- How will volunteer healthcare providers know where to supply this information during a disaster?

PROTECTING HEALTH INFORMATION

Paper Record Transfers

In the event that EHRs are not available, paper will be used to document patient care. Processes need to be in place to address paper records going with patients when they are triaged to other facilities and how they will be packaged for return after care is completed. This scenario should be placed in disaster training exercises with a process created.

HIPAA and Privacy and Security

The key requirements in the privacy rule include directory information. The rule provides for disclosure of directory information (name, location, and condition) for all patients unless they opt out in favor of greater privacy.[4] Guidance from the Office for Civil Rights (OCR) states that unless there is compelling evidence otherwise, organizations can assume that patients wish to be included in the directory even if they are not able to indicate that directly. In a disaster setting this certainly may be assumed to be true for all patients. [5]

The OCR guidance provides that in an emergency situation, PHI may be shared without authorization with disaster relief organizations that are authorized by law or chartered to assist in disaster relief efforts, even though such agencies are not covered entities and are not bound by any re-disclosure constraints. Such sharing enables victim identification and ultimately the reuniting of families and other social groups.[6]

HIPAA requires health plans, healthcare clearinghouses, and healthcare providers that maintain or transmit health information electronically to provide reasonable and appropriate administrative, technical, and physical safeguards to ensure the information's integrity and confidentiality. These covered entities protect the information against any reasonably anticipated threats or hazards to its security, integrity, or unauthorized use and disclosure.[7] HIPAA also allows a covered entity to use or disclose protected health information to a public or private entity authorized by law or by its charter to assist in disaster relief efforts to coordinate family notification efforts.

Applicable federal and accreditation requirements should be referenced when developing a disaster plan.

Use and Disclosure/Release of Information

Even where a stricter state law pre-empts HIPAA and requires authorization prior to disclosing personal health information (PHI) for treatment, any PHI necessary for treatment may be shared in an emergency without authorization.

If a patient has a personal representative, PHI may be shared with that individual as if he or she were the patient. In the absence of a personal representative the minimal amount of information necessary may be shared with an individual caring for a patient to the extent that it is necessary to provide such care.[8]

Disclosure of PHI may be made to any individual directly involved in assisting the patient in making payments or resolving a payment issue, including a relative, a friend, or even a public official; provided there is indication that the patient has requested the individual to intercede or it is in the patient's best interest to do so.[9]

A business associate acting on behalf of a covered entity may disclose PHI to the extent permitted in its business associate agreement. The associate may also subcontract with an agent who may function in accordance with the terms of the signed agreement provided that the business associate ensures that the agent agrees to the provisions of the agreement. An agreement must be drawn up and signed to attest to this.[10]

Although covered entities are still obliged to protect the confidentiality of PHI to the extent possible, OCR outlines additional permissible uses and disclosures in various bulletins to prevent inappropriate use and disclosure and to limit access to the minimum necessary to accomplish the necessary task at hand and meet the exigencies of a disaster.

According to OCR, PHI may be shared without authorization to prevent serious harm to the patient or to the public while the disaster is ongoing.[11] During the disaster the covered entity and its business associate may amend the agreement to the extent necessary.[12]

For the purpose of providing or enabling care, health plans and providers may share prescriptions or other PHI with providers at shelters.[13] If a provider is not able to formalize a business associate agreement due to the grave nature of a disaster, disclosure may be made for care or identification purposes as if the agreement were executed, provided that an agreement is executed as soon as practically possible.[14]

Note: For more information on disclosure of individually identifiable health information in emergency situations the Office for Civil Rights (OCR) provides guidance and several bulletins regarding emergency response, planning and preparedness on their website. Readers should reference this guidance in their planning activities.

Requesting a Waiver

The HIPAA privacy rule is not suspended during a national or public health emergency. The secretary of HHS may waive certain provisions of the rule under the Project Bioshield Act of 2004 and section 1135(b)(7) of the Social Security Act.[15]

Contact the regional and national OCR offices to inquire about a HIPAA waiver and its use in your particular situation.

The Joint Commission

The Joint Commission has an established "Emergency Management (EM)" section in the accreditation requirements for hospitals.

These standards require planning activities, an emergency operations plan, how it will communicate, how it will manage resources, assets, security, safety, staff, utilities and patients during an emergency. The standards also addresses granting emergency privileges, assigning disaster responsibilities to volunteer practitioners, a self-evaluation of the effectiveness of said planning activities, and the emergency operations plan.

RECOVERY

EVALUATION, INVENTORY, AND RECOVERY PLANS

The post-disaster recovery planning phase serves several key purposes:

- Evaluating the crisis and the response is helpful not only to the organization, but also serves as a learning tool for other facilities.
- Follow-up plans assist in the recovery of the organization and also the participants in the crisis response. These plans should include assessing the damages and beginning to determine what repairs are needed.
- A thorough inventory and assessment of types, location, and volume of damaged and/or missing PHI including:
  - Paper charts
  - Films and other medical imaging media
  - IT infrastructure of information not backed up or compromised due to the disaster
  - Off-site paper charts and records stored at remote location
  - Other files such as legal, personnel, or committee work, and any electronic system containing PHI

Issues that should be included in the recovery plan include:

- Emergency services including law enforcement and fire department personnel to be on-site
  - Inspections that will take place to ensure proper code, standards, and other activities.
  - From this assessment, determination can be made as to which equipment and records can be recovered.
- Designating a person in charge of recovery
- Facility cleanup and support
- Record preservation and financial billing of individuals treated
- Salvage, waste, and garbage disposal

After the critical phase has passed, attention will turn to management of the data created during the crisis. It is critical to perform an "autopsy" of the documentation process and conditions.

The data autopsy should include:

- All decisions made regarding management of data
- What documentation was created
- What type of systems were used to create information and data
- The scope of the emergency measures implemented, including the time frame within which the disaster occurred, the number of patients treated, and to the extent possible, staffing schedules

Based on feasibility and a risk-versus-benefit decision-making process laid out in the disaster plan, the following decisions must be made:

- Whether to integrate or segregate documentation created during the disaster based on the anticipated ease of future access to the patients' designated record sets
- Whether resources should be allocated to flesh out documentation of demographics, diagnoses, signatures, or discharge summaries

Recovery of destroyed or damaged documents requires careful assessment. To the extent records cannot be reconstructed by means of either electronic data recovery, retrieval from an affiliated HIE, or through a damage restoration company, evaluate the following to reconstruct as much data as possible:

- Re-transcribing documents, if voice file still exists
- Acquiring documentation from source systems or referring physicians if they were not damaged, including documents from third-party vendors and HIE if applicable.
- Costs associated with recovery, including restoration of systems where backups are available and including estimated time to recreating records
- Acquire documents from any undamaged databases, such as admission, transcription, laboratory, and radiology databases or data backup services
- Obtain copies from recipients of previously distributed copies, such as physicians' offices, other healthcare facilities, or the business office
- When unable to reconstruct part or all of a patient's health information, document the date, the information lost, and the event precipitating the loss in the patient's record

Reconstruction of information must be documented, including the method used, and the entry must be authenticated according to the organization's policy.

DEBRIEFING

For compliance, performance should be carefully evaluated alongside the original plan to ascertain lessons learned and corrective action needed for the future.

Questions to ask include:

- In what areas did expectations exceed the plan?
- What actions could be improved?
- Were there any drawbacks in responses?
- What additional actions would be needed to make the plan more effective?
- Was there a failure to follow the plan, and if so, why?

To determine corrective action for the future, ask:

- Does the plan need to be updated?
- Should backup provisions be improved or extended?
- Is the data management plan realistic (i.e., does the decision to integrate or segregate disaster data mesh with reality and long-term strategy)?

Finally, based on the conclusions reached, the organization should develop procedures for testing and revising contingency plans.[16]

With careful planning, objective evaluation and re-evaluation, it is possible to make the best of the situation. Clearly, saving life or limb trumps privacy, but not even disasters justify wanton disregard of patient privacy rights. If it is possible to preserve only a shred of privacy, that shred should be preserved to provide the patient with whatever dignity is possible.

MATCHING AND TRACKING TESTS

A recovery plan should assume that patient management and care can begin to suffer immediately upon the disaster event. The electronic system's capability to transfer patient information will quickly degrade in times of electrical disturbances. In the event of a paper record, or hybrid record some medical information can be lost forever.

For the organization to effectively recover from a disaster or unplanned interruption to its information and revenue cycle services:

- A pre-determination by senior leadership must earmark funding to maintain these system operations.
- Planning for these events must take into account that victims will report to the hospital immediately after the disaster.
- During this time, the organization may be reduced to a paper health record until a total system recovery is completed.
- Organization must have guidelines surrounding how hospital charges will be collected during this time period.
- HIM departments must collaborate with other departments to plan for the processes of updating records with patient identifiers and assisting with the billing process.

RECORD PRESERVATION

Establish and maintain relationships with equipment and supply vendors immediately if they are not already formed. These relationships will streamline the process of obtaining equipment and supplies during the disaster period.

Areas where prior arrangements with vendors may be necessary include data and record recovery, physical retrieval, recovery, cleaning, freeze-drying and mold elimination as well as fire, water, and storm damage restoration services.

Develop written agreements with potential disaster recovery vendors or alternative service providers and locations as needed.

Contracts for damage restoration services must provide that the services will be performed in accordance with the HIPAA privacy and security rules for business associates. The contract should specify:

- Method of recovery
- Nonuse or further disclosure of the information other than as permitted or required by the contract
- Use of appropriate safeguards to prevent use or disclosure of the information other than as provided for by the contract
- Reporting to the contracting entity any inappropriate use or disclosure of the information of which it becomes aware
- Ensuring that business associate agreements are initiated with any subcontractors or agents with access to the information agree to the same restrictions and conditions
- Indemnification of the healthcare facility from loss due to unauthorized disclosure
- Report to the covered entity any use or disclosure of PHI not provided for by its contract, including breaches of unsecured PHI
- Return of the information at the termination of the contract or provision of a certificate of its destruction and assurance that the contractor retains no copies
- Time that will elapse between acquisition and return of information and/or equipment
- Authorization of the contracting entity to terminate the contract if the business partner violates any material term of the contract

AUDIT, CONTROL, AND MAINTENANCE

Once a disaster strikes and the disaster response plan is executed, post-disaster management is crucial.

Documentation is a key final step in any disaster plan. The facility must prepare a detailed record of the disaster event that includes at minimum a list of patient records affected, recovery efforts taken, and outcomes. Organizations also should maintain a log of lost or destroyed records, which will allow for easy retrieval of general information regarding the past event should any legal or accreditation issues arise.

If a facility discloses patient information that has portions missing or reconstructed due to a disaster, it must include with the record a copy of the entry documenting the loss or reconstruction.

Another key step to post-disaster management is to meet with staff and communicate. Staff should be given the opportunity to provide input to help evaluate departmental performance and identify opportunities for improvement. Most importantly, keep in mind that staff may need time for the grieving and healing process that follows emotionally charged disasters.

The loss of health information can cause delays in patient care, missed medications, or numerous other healthcare crises. Supporting the continuum of care and providing a longitudinal record that can follow a patient throughout the course of his or her life is important to every organization. By appropriately planning in advance for disaster, organizations can mitigate potential healthcare concerns and provide patients with valuable information in the aftermath of a disaster.

NOTES

1. National Institute of Standards and Technology. "Guide for Conducting Risk Assessments." Special publication 800–30, September 2012. http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf.
2. Department of Health and Human Services. "Security Standards for the Protection of Electronic Protected Health Information." 45 CFR part 164, subpart C, 164.308. *Code of Federal Regulations*, 2003. http://www.gpo.gov/fdsys/pkg/CFR-2007-title45-vol1/pdf/CFR-2007-title45-vol1-part164.pdf.
3. Zigmond, Jessica. "Obama Inks Hazard Preparedness Legislation." *Modern Healthcare*, March 13, 2013. http://www.modernhealthcare.com/article/20130313/NEWS/303139943
4. "Health Insurance Portability and Accountability Act of 1996 (HIPAA)." Public Law 104-191. http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/.
5. Department of Health and Human Services, Office for Civil Rights. "HIPAA Privacy Rule Compliance Guidance and Enforcement Statement for Activities in Response to Hurricane Katrina." Hurricane Katrina Bulletin #2, September 2, 2005. http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/emergency/enforcementstatement.pdf.
6. Ibid.
7. "Health Insurance Portability and Accountability Act of 1996." Public Law 104–191, Title II, Subtitle F, Section 262, Part C, Section 1172-73. August 21, 1996. http://aspe.hhs.gov/admnsimp.
8. "Privacy of Individually Identifiable Health Information." *Code of Federal Regulations*, 2002. 45 CFR part 164, section 510(b). http://www.gpo.gov/fdsys/pkg/CFR-2007-title45-vol1/pdf/CFR-2007-title45-vol1-part164.pdf.
9. Office for Civil Rights. FAQ #1067, March 14, 2006.
10. Department of Health and Human Services. "Privacy of Individually Identifiable Health Information: Uses and Disclosures—Organizational Requirements." *Code of Federal Regulations*, 2002. 45 CFR part 164, section 504(d)(2)(ii)(D). http://www.gpo.gov/fdsys/pkg/CFR-2007-title45-vol1/pdf/CFR-2007-title45-vol1-part164.pdf.
11. Department of Health and Human Services, Office for Civil Rights. "HIPAA Privacy Rule Compliance Guidance and Enforcement Statement for Activities in Response to Hurricane Katrina."
12. Ibid.
13. Ibid.
14. Ibid.
15. Office for Civil Rights. "Is the HIPAA Privacy Rule suspended during a national or public health emergency?" http://www.hhs.gov/ocr/privacy/hipaa/faq/disclosures_in_emergency_situations/1068.html.
16. Department of Health and Human Services. "Security Standards for the Protection of Electronic Protected Health Information." 45 CFR part 164, subpart C, 164.308(a)(7)(ii)(D). Code of Federal Regulations, 2003. http://www.gpo.gov/fdsys/pkg/CFR-2007-title45-vol1/pdf/CFR-2007-title45-vol1-part164.pdf.

REFERENCES

For more information, please see AHIMA's disaster planning and recovery resources in the AHIMA Body of Knowledge or at myphr.com.

Centers for Disease Control and Prevention. "What Is a Traumatic Event?" June 12, 2003. http://www.bt.cdc.gov/masscasualties/copingpro.asp.

Centers for Medicare & Medicaid Services (CMS). "Additional Editing for Disaster Related Claims." Pub. 100–20, Transmittal 809, November 12, 2010. http://www.cms.gov/Regulations-and-Guidance/Guidance/Transmittals/downloads/R809OTN.pdf.

CMS. "Additional Emergency and Disaster-related Policies and Procedures That May Be Implemented Only with a 1135 Waiver." January 31, 2013. http://www.cms.gov/About-CMS/Agency-Information/Emergency/downloads/MedicareFFS-EmergencyQsAs1135Waiver.pdf.

CMS. "Requesting an 1135 Waiver." November 4, 2009. http://www.cms.gov/About-CMS/Agency-Information/H1N1/downloads/RequestingAWaiver101.pdf.

Emergency Planning and Disaster Recovery Sourcebook. 19th ed. Ashton, MD: Edwards Information, 2011.

Federal Emergency Management Agency (FEMA). "Community Emergency Response Teams." http://www.fema.gov/community-emergency-response-teams.

FEMA. "Family Emergency Plan." http://www.ready.gov/sites/default/files/FamEmePlan_2012.pdf.

Government Emergency Telecommunications Service. http://gets.ncs.gov/

Office for Civil Rights. "Can health care information be shared in a severe disaster?" http://www.hhs.gov/ocr/privacy/hipaa/faq/facility_directories/960.html.

Office for Civil Rights. "Health Information Privacy." http://www.hhs.gov/ocr/privacy/index.html.

Office of the Assistant Secretary for Preparedness and Response. "Public Health Emergency." http://www.hhs.gov/ocr/privacy/index.html.

Pandemic and All-Hazards Preparedness Reauthorization Act of 2013. Public Law 113-5, 113th Congress (March 13, 2013). http://www.gpo.gov/fdsys/pkg/PLAW-113publ5/pdf/PLAW-113publ5.pdf.

APPENDIX A

SAMPLE CONTINGENCY PLAN:

This sample plan includes:

- A Disaster Plan Development Checklist
- Contingency Plan (includes plan solutions and alternatives, tasks to be performed for selected alternatives and contact list)

	Sample Disaster Plan Development Checklist: ***For each plausible disaster and major function, develop a contingency plan. As plans are completed and/or updated, place a check mark in the corresponding box.**						
	Major Function	**Extended Power Outage**	**Fire**	**Flood**	**Hurricane**	**Manmade Disaster**	**Other**
1	Master patient index (MPI)						
2	Assembly						
3	Deficiency analysis						
4	Coding						
5	Abstracting						
6	Release of Information						
7	Transcription/Dictation						
8	Chart tracking, location, and provision						
9	Birth certificates						

SAMPLE CONTINGENCY PLAN

Facility name:

Department name:

Plan originator:

Date:

Major function: Maintenance of an accurate MPI

Disaster: Extended power outage

Assumptions: An ice storm has resulted in an extended power outage with the hospital operating on generator or backup power. Most staff members are able to report to work.

Existing process detail: Under normal circumstances, the MPI is generated through entries made by registration and admitting staff and contains detailed patient information, including the patient's name and medical record number. When a patient is registered, the admitting and registration staff access the electronic MPI to determine whether the patient already has a medical record number or whether a new number must be generated. HIM staff also may access the MPI for various functions, such as when they need a medical record number to pull medical records for a current hospitalization, to accompany a bill for payment, for continuing care, for quality monitoring or legal action, and to number documents for placement in the paper record. The accuracy of the numbers assigned is verified by HIM. Without power, this process will not be able to be performed.

If/then scenarios: If admitting and registration staff do not have access to the MPI when registering a patient, then the following might result: the registration system or registrars will assign new numbers, creating duplicates that may cost $20 per set to correct, or the registrars will issue no numbers and patient health information will have to be matched to patients by using account numbers, admission or discharge dates, or birth dates. Medical record numbers will have to be assigned and entered into the database at a later date.

If HIM staff members do not have access to an MPI, then record retrieval for patient care and other healthcare-related purposes cannot occur.

Interdependencies: Information technology (IT), registration staff, patient care areas, document imaging, transcription, billing, and external customers, including patients, third-party payers, attorneys, and regulatory agencies, need the medical records, so a functional MPI is required.

Contingency Plan Solutions and Alternatives		
Potential Solutions/Alternatives	**Limitations**	**Benefits**
Auxiliary power will be used to access an electronic copy of the MPI on disk	• MPI won't work without auxiliary power • The process is cumbersome • This process will likely generate some duplicate medical record numbers • It is costly for human resources to correct duplicate numbers	• Admitting staff are accustomed to this process • Process produces fewer duplicates than with no back-up system • Process is less cumbersome than a totally manual system
Staff members will have to depend on a paper MPI	• Printouts will be cumbersome • Printouts probably will be located in HIM • The process will likely generate duplicate or no numbers • It is costly for human resources to use manual system and correct duplicate numbers	• Process provides a mechanism to look up a patient's number and pull a chart when critical

Contingency Plan Tasks to Be Performed for Selected Alternatives (before, during, and after disaster)	
Activity	**Responsibility**
Verify availability of MPI on disk	Associate Director, HIM
Implement processes to update disk daily	Associate Director, HIM
Develop contingency plan procedures and training materials	Associate Director, HIM
Train admitting and registration and HIM staff to use contingency plan	Associate Director, HIM
Use post-disaster and implementation contingency plan	Data Quality Coordinator, HIM
Schedule production and delivery of paper MPI routinely	Associate Director, HIM
Create contingency procedures and training materials for manual system	Associate Director, HIM
Develop schedule to update contingency plan and training materials	Associate Director, HIM

Contact List	Phone Number	Service Provider
HIM Director		
HIM Assistant Director, Manager, Supervisor		
HIM Staff Members		

APPENDIX B

SAMPLE STAFF COMPETENCY LIST
SAMPLE RELEASE FORM

Sample Staff Competency List

Facility Name
Health Information Disaster Plan
Staff Competency Checklist

Staff Member Name:_____Date:_____

	Yes	No
1. Staff member demonstrates familiarity with the disaster manual by quickly locating various disaster protocols and emergency phone numbers. This type of information could be stored in "grab bags" for staff to locate when preparing for disaster.		
2. For each plausible disaster type, staff member accurately verbalizes the contingency plan.		
3. For each plausible disaster type, staff member accurately verbalizes or demonstrates his or her own responsibilities.		
4. Staff member can articulate methods of protecting people, health information, and equipment from damage.		
5. Staff member accurately verbalizes transportation and storage options for relocating equipment and health information.		
6. Staff member knows to wear identification badge when called back to work during a disaster.		
7. Staff member knows how to contact supervisor or manager via text or social media if phone are out for an extended period of time.		

APPENDIX C

IMMEDIATE AND SHORT-TERM CONCERNS CHECKLIST

Immediate Concerns
• Mobilization of internal communication plan and community-wide disaster plan if applicable   • Check flashlights, emergency lighting, general electric (i.e. air conditioning, heat)

• Account for staff and address immediate needs:
  • Use radio and television public-access channels to communicate announcements
  • Implement department phone tree (i.e. director calls two people who each call two people) or automated notification system to account for all employees
  • Notify employees to either report to work or stay at home
  • Can also be used for other pertinent personnel such as contractors and vendors.
  • Maintain in paper and electronic forms
  • If Internet is available, consider e-mail and social media as means to communicate with employees
  • Provide provisions to staff that may be stranded due to lockdown, martial law, or environmental barriers to gaining access to the facility (e.g., safe sleeping areas, shower and restroom facilities, food and water)
  • Remind staff where to locate, how to access protected health information (PHI) as well as ensure that it is properly labeled during the downtime situation.

• Check availability of communication devices; phones (land lines and cell phone), internet
  • Consider use of two-way radios
  • Plan for recharging phones and usage
  • Consider creating a contact list that distinguishes the cell phone provider. If one particular provider has been affected, the list may aid in identifying those staff members who may not have cell phone access.

• If there is no power, there will be no way to copy or scan records, or gain access to the EHR:
  • Prepare process for patients transporting original records to other healthcare facility
  • Implement appropriate EHR downtime procedures
  • Work with other hospitals and clinics in your area on inventory of received records and the return process
  • If EHR is unavailable when power is restored, the fax line can serve as the primary means of electronic communication whereby information can be sent and received from other facilities
  • Institute setup for incoming patients to the emergency department (ED)
  • Every patient will need a manually assigned encounter number (consider pre-made charts stored in secure off-site location and a backup plan if the site cannot be reached)

• Consult with Human Resources on personnel policies and communicate to staff:
  • Work and payroll schedules, benefits, and use of vacation time, sick time, FMLA, etc
  • Roles and responsibility changes due to limited staff availability related to a variety of circumstances.
  • Remind staff to wear identification badges when reporting for work.

Short-Term Concerns

• Use press coverage (radio/public access television/Internet) to relay process for retrieving, disposal, or returning of information. Considerations for the communication:
  • Directing the public to inspect the information for PHI
  • If the documents or film do not have any PHI, consider directing the public to destroy it by shredding, cutting into very small pieces, or burning
  • If the documents or film have PHI (name, date of birth, address, social security number or other identifiable number(s), phone number, or a combination of these), direct the public to return the information. Suggestions include:
  • First try to determine how far the information traveled due to the disaster
  • If your healthcare system has other locations in the area, consider having the information sent to the privacy officer at that location
  • If your healthcare system is a stand-alone hospital, consider setting up a PO Box at a local post office, mailing company, or other designated location and post the Privacy Officer's contact information
  • Provide options of delivering the information vs. mailing the information and consider paying the postage cash on delivery (COD) or ask that the sender place a request for the reimbursement with the returned documents, including their name and address where the refund can be mailed

• Notify Regional and National Office for Civil Rights (OCR) office:
  • Obtain clarification on handling records
  • Ask if press coverage will satisfy the >500 notification rule
  • Inquire about HIPAA waiver and its use in your particular situation

• Notify:
  • The Joint Commission and other pertinent accrediting agencies
  • Business Partners and other pertinent governmental agencies

• Inventory and assessment of types, location and volume of damaged and/or missing PHI including:
  • Paper charts
  • Films (x-rays)
  • IT infrastructure (information not backed up or compromised due to the disaster)
  • Off-site paper charts stored at third-party vendor location
  • Off-site record location owned by facility; determine status of building
  • Legal files, personnel files, committee minutes
  • All electronic systems containing protected health information (PHI)

• Assess reconstruction of documents that were damaged or lost in the disaster:
  • Explore recovery of documents:
  • Previously imaged by contracted third party vendors who provide on-site services (such as document management or release of information)
  • Previously distributed copies to providers and other healthcare facilities not affected by the disaster
  • Calculate costs associated with recovery including estimated time to recreate records
  • Restoration of systems where a backup is available
  • If source systems are available, may be able to re-send, (e.g., transcription, labs, radiology)
  • Re-transcribe documents left in dictation system

APPENDIX D

SAMPLE
EMERGENCY PRIVILEGE APPLICATION AND RELEASE FORM
PHYSICIANS AND ADVANCED PRACTICE PROFESSIONALS

Physicians and Advanced Practice Professionals
Application for Disaster Credentialing

Date: _____

Name: _____
Last First Middle Professional Title (MD/DO/DDS/DMD/DPM/APN/PA/PsyD

_____
Specialty Social Security Number Date of Birth

State Professional License/Certification Number: _____ Expires: _____

DEA Number: _____ Expires _____

Professional Liability Insurance Carrier: _____

Policy Number: _____ Dates of Coverage: From: _____ MM/YY To: _____ MM/YY

Current Primary Affiliation/Hospital: _____

State Driver's License Number: _____ Expires: _____

Practitioner's Office Address: _____

Office Telephone: _____ Office Fax: _____

Home Telephone: _____ Cell Number: _____

Medical/Professional School and Date(s): _____

Verifications Log: Information must be verified within 72 hours

FOR HOSPITAL USE ONLY

Copy of Photo ID obtained for file (as feasible) Identified by Medical Staff Member: _____

Practitioner Assigned ID Badge by: _____
Name Date Department

Practitioner Granted Disaster Privileges on: _____ By: CEO/President and/orChief of Staff/Designee

Dept/Specialty: _____ Notified Via: _____ Initials: _____

Assigned to Medical Staff Member (name): _____

Current Licensure/No Restrictions ☐ Yes ☐ No Date Verified: _____ Via: _____ Initials: _____

BNDD License: Date Verified: _____ Initials: _____ Number: _____

Hospital Affiliation /
No Privilege Restrictions: Specialty: _____ Date Verified: _____ Via: _____ Initials: _____

NPDB Query Date: _____ Initials: _____ Report Received/Reviewed: Date: _____ Initials: _____

Adverse Information: ☐ Yes ☐ No NPDB Report: _____

Malpractice Insurance Verified: Date: _____ Via: _____ Initials _____

Practitioner Temporary Scope of Practice End Date:

SAMPLE RELEASE FORM

I, _____, certify that I am licensed/certified as a _____, in the state of _____, license # _____, with no restrictions on clinical privileges at any hospital now or in the past.

I hereby volunteer my medical services to (organization) _____ during this disaster and agree to practice as directed and under the supervision of a member of the medical staff of (organization) _____. I agree to wear my ID badge issued by (organization) at all times when functioning under temporary privileges to enable staff and patients to readily identify my status.

I also acknowledge that my temporary disaster privileges at this facility shall immediately terminate once the disaster has ended, as notified by the facility, and that these privileges may be terminated at any time without cause or reason and without right to a hearing or review.

All health information is the property of (organization) and is maintained to service the patient, healthcare providers, and the institution in accordance with legal, accrediting, and regulatory agency requirements. All patient care information is regarded as confidential and will be available only to authorized users. Patients have a right to privacy and any unauthorized disclosure by you of confidential information may result in possible legal action.

(Signature of Practitioner) Date _____

(Signature of Organization's Medical Staff Member) Date _____

Recommending Privileges—If applicable)

The information as provided by the practitioner has been reviewed and verified, as possible, by Medical Staff Services. On this basis, this practitioner is hereby granted temporary disaster privileges to treat patients presenting to (organization) _____ during this declared emergency/disaster.

Signature of CEO/President

and/or Chief of Staff (or designee) _____

Date _____