EMPOWERING PEOPLE TO IMPACT HEALTH

Disaster Planning and Recovery

Toolkit

AHIMA
American Health Information Management Association®

ISBN: 9781584265634

AHIMA Product No.: ONB202016

AHIMA Staff:
Rachel Schratz, Assistant Editor
Megan Grennan, Managing Editor
James Pinnick, Sr., Director Publishing

Limit of Liability/Disclaimer of Warranty: This book is sold, as is, without warranty of any kind, either express or implied. While every precaution has been taken in the preparation of this book, the publisher and author assume no responsibility for errors or omissions. Neither is any liability assumed for damages resulting from the use of the information or instructions contained herein. It is further stated that the publisher and author are not responsible for any damage or loss to your data or your equipment that results directly or indirectly from your use of this book.

The websites listed in this book were current and valid as of the date of publication. However, webpage addresses and the information on them may change at any time. The user is encouraged to perform his or her own general web searches to locate any site addresses listed here that are no longer valid.

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

Back to TOC

FOREWORD

In a disaster, health information must be protected to ensure it is secure, reliable, and accessible, and that it supports the patient's continuum of care. Business disruptions, both planned and those due to unplanned disasters, are likely to impede the availability of electronic health records (EHRs) and other information technology (IT) assets; rendering them unavailable to clinicians and other workforce members for day-to-day business operations. Forward-thinking disaster planning benefits the overall recoverability and resiliency of a healthcare organization.

The Disaster Planning and Recovery Toolkit addresses these requirements with emphasis on capture of documentation of patient care rendered during a disaster, the proper communication, relaying of diagnostics, treatments, and care planning among caregivers and patients, data backup plan availability as well as the integrity of healthcare information.

This toolkit assists in this process by providing a sample contingency plan, sample staff competency list, and an outline of useful tips for implementation. In addition, it also outlines steps necessary for a data backup plan to address data availability as well as the integrity of the information needed by the healthcare organization, and it outlines elements of a functional back up plan and data recovery principles.

As an HIM leader, it will be helpful to keep some key information from this toolkit with you in case a disaster occurs when you are away from the facility. While this toolkit focuses on the HIM services primarily, it is strongly encouraged that the HIM disaster operations are coordinated and integrated with the organization's overall Disaster Response Plan as well as the IT Business Continuity Plan.

AUTHORS AND ACKNOWLEDGEMENTS

Authors

Nancy Davis, MS, RHIA, CHPS; Elisa R. Gorton, MAHSM, RHIA, CHPS, CHC; Cynthia Leonhard, RHIA, CHTS-TR, MJ; Susan M Lucci, RHIA, CHPS, CHDS, AHDI-F; Brenda Olson, MSEd, CHP, RHIA; Grissel Pabon Reyes, MS, RHIA, CDIP, CCS, CCS-P; Roger Shindell; Robyn Stambaugh, MS, RHIA; Linda Renn, RHIT, CHPS, CCS, CPC, COC, CHTS—TR; and Vivian Thomas, RHIA CHDA CPHQ CHPS CDIP

Acknowledgements

Nicole Neidig; Jill Flanigan; Pamela Varhol; Patricia Buttner, MBA/HCM, RHIA, CDIP, CHDA, CPHI, CCS, CICA; Twanna Huffman; Margie Stackhouse, RHIA; Diana Warner, MS, RHIA, CHPS, CPHI, FAHIMA; Lori L. Richter, MA, RHIA, CPHIT, CPEHR, CHPS; Donna J. Rugg, RHIT, CDIP, CCS-P, CICA, CCS; Maggie Foley; Chris Apgar; Julie A. Dooling, MSHI, RHIA, CHDA, FAHIMA; Laurie Peters, RHIA, CCS; Tammy Combs, RN, MSN, CCS, CCDS, CDIP; Mona Calhoun, MS, M.Ed, RHIAFAHIMA; Lyn Rossman; Ann Meehan, RHIA; Karen Searcy, RHIA, CPC; Linda D. Williams; Kelly McLendon, RHIA, CHPS; Crystal A. Clack, MS, RHIA, CCS, CDIP; Dana DeMasters; and Jami Woebkenberg, MHIM, RHIA, CPHI, FAHIMA

Previous Authors

Julie A. Dooling, MSHI, RHIA, CHDA, FAHIMA; Theresa Rihanek, MHA, RHIA, CCS; Diana Warner, MS, RHIA, CHPS, FAHIMA; and Lou Ann Wiedemann, MS, RHIA, CDIP, CPEHR, FAHIMA

Previous 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; and Lydia Washington, MS, RHIA, CPHIMS

Original Authors

Jill Burrington-Brown, MS, RHIA; Patricia Cunningham, MS, RHIA; and 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, healthcare facilities in the United States have experienced natural and man-made disasters. The range of impacts to a healthcare organization can be from an overwhelming influx of patients requiring emergency care, a massive power outage that restricts electronic resources, shutdown of the essential EHR system, and destruction to the physical property of the health facility. As a result, disaster planning, preparedness, business continuity operations, and recovery efforts have come to the forefront for health information management (HIM) and healthcare enterprises 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.

HOW TO USE THIS TOOLKIT

The purpose of this toolkit is to provide a guide to health information leaders on how to prepare for a disaster and to be an active participant in an organization's disaster response plan. As HIM leaders, it is our responsibility to ensure health information is available and managed securely. Those same standards apply to patient information obtained during and following a disaster.

This toolkit offers a variety of preparedness business guidance, checklists, and references that HIM professionals can use to perform self-assessments with an eye toward improving preparedness. It also provides information on external preparedness checklists and toolkits, the hyperlinks to these resources, and the name of the source organization.

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 that may impact healthcare delivery.

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 a pandemic "infectious disease outbreak." A pandemic incidence could require organizations to implement disaster protocols with potential lack of availability of sufficient staff requiring external assistance to handle the influx and management of patients. A pandemic 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 cyber-attacks or threats on the healthcare facility's EHR and communications system. 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 health record (EHR) systems.

ADVANCE PLANNING FOR POTENTIAL DISASTERS

Creating the Business Continuity Plan (BCP)

Access to medical services, past health information about an individual's health status, and health records serve a vital function during disasters. The 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 critical operations and access to information more efficiently in the event of disaster.

Per the requirements of accrediting and licensing organizations and Federal HIPAA (Health Insurance Portability and Accountability Act) regulations, every organization must have a comprehensive plan that protects patient safety, secures health information from loss or damage, ensures stability in continuity of care, 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 must be championed and funded by senior management and involve an interdisciplinary team, including all impacted departments and stakeholders. Team members must commit adequate time and senior management must commit adequate resources to the process.

A BCP should address:

- The relationships with local and community emergency response teams and agencies.
- Understanding how responses to the disaster will be evident through planning, drilling, and teamwork both inside and outside the organizations, including community involvement, is essential.
- Partnerships with community planners, public health department, state hospital associations, and local medical societies.
- Training protocols both internally and in conjunction with community response teams, as necessary.

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 health records or health information, including the Office of the National Coordinator for Health Information Technology, the Centers for Medicare and Medicaid Services (CMS, and 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
- Discussions with the regional health community and colleagues who have experienced the types of disasters anticipated by the facility
- Determining to what extent the facility's insurance covers the costs associated with disaster planning such as transport of health information, relocation (including over state lines), recovering damaged information, and lost revenue caused by the inability to restore information

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 of needs
- Downtime and contingency planning
- Business operations continuity during the disaster (emergency mode operations)
- Disaster recovery and care documentation databackup

Risk Assessment and Analysis of Needs

A risk assessment must 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 and the impact such an occurrence will have on the organization and their patients. 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 analyses focus on applications, the information systems supporting the applications, and the physical security surrounding those assets. An assessment of the safeguards governing operational practices such as policies, procedures, responsibilities, and training would also be included in a thorough risk analysis.

HIPAA and some accrediting agencies include requirements for risk assessments. HIPAA calls for organizations (covered entities (CEs) and business associates (BAs)) to create a plan to follow when disaster strikes. The first step is to conduct a risk assessment to profile those critical components and prioritize those components to include in the BCP. 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 may collaborate with other stakeholders involved with the security of the facilities and the IT system to ensure key processes and systems that support the EHR system. Across the essential HIM domains of patient registration, document management, coding of diagnoses and procedures, release of medical information, transcription, and billing, disaster impacts are assessed and any identified risks are appropriately addressed.

In July 2016, the Office of the National Coordinator for Health Information Technology (ONC) published the Safety Assurance Factors for EHR Resilience (SAFER) guides. The section in the Contingency Planning SAFER Guide “identifies recommended safety practices associated with planned or unplanned EHR unavailability.”[1]

In addition, considerations must be given to any system that may exist outside the proverbial four walls of the organization such as business associates, health information exchanges (HIEs), and other third-party vendors that receive or share PHI. 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 in addition ti preparing for and conducting a risk assessment.[1]

Downtime and Contingency Planning

For contingency planning, whether it is an unintentional manmade or natural disaster, make a list of the various types of disasters that are specific to both the location and facility that might directly impair the operation of the facilities, such as fire, explosion, tornado, hurricane, flood, earthquake, severe storm, bioterrorism, cybersecurity/security incident, or extended power failure, etc.

Next, list the HIM department's core processes. For example, this may include maintenance of an accurate master patient index (MPI), coding, document management and imaging, clinical documentation improvement, release of information, revenue cycle, transcription, and EHR documentation and reporting. Also, consider listing department core processes which involve healthcare documentation and user workflow impacts such as physician progress notes and orders, legal care consent management, nursing notes and medication administration recording, laboratory order and resulting, medication order entry coordination with pharmacy, and other diagnostic and treatment documentation. For each plausible disaster and core process, generate a contingency plan. (See Appendix A, "Sample Contingency Plan.")

The HIPAA security rule applies to electronic protected health information (PHI) only; however, in order to comply with the privacy rule, backup and recovery of all PHI must be provided, 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]

Disaster Recovery Plan

Disaster recovery is a plan that is a subset of business continuity. This part of the 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 determine how crucial decisions are reached. For example, in a potential disaster, solutions must already be defined and practiced surrounding critical action steps that must be taken swiftly to ensure continuity of care and business operations. Consider the following:

- Are downtime procedures ready and accessible for immediate implementation in all care provider locations?
- Will this disaster require a potential evacuation of some or all patients, and how will relocation of patients be tracked in absence of the EHR?
- What is the estimated time of arrival to resumption of full operations, or is the plan sustainable over an extended period of time (weeks)?

The plan should also account for the physical security of the premises, since depending upon the type of disaster, the perimeter of the premises will be secured. If the facility has experienced structural damage, flooding, or if an evacuation has been ordered, security measures must be in place to prevent 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 manually documenting concurrent clinical findings and treatment rendered during the disaster in a manner that will be retrievable after the disaster recedes.

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 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.

"View only" backup access, differentiated from the live/production access for the EHR system, should be in place in every location where care is rendered in the healthcare facility, for care providers to access past medical data regarding care rendered, medications, patient history and status, laboratory and imaging records and results. Also, the HIM services must have "view only" backup access for the essential domain of the release of medical information to patients, care providers, and authorized third-party requestors for health records during the disaster.

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, and steps for securely restoring all components of the health informationsystem
- 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 rebuilding data tables, restoring access to 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, the PHI must be restored in a usable format in a relatively quick and efficient manner. Standard data recovery principles that uphold the practices of confidentiality, integrity, and accessibility (CIA) should be applied during the planning and back-up periods, including:

- Provisions for reading data created during the downtime process on applications or paper are later transitioned into the EHR/legal healthrecord
- Implementing legally required data retention policies with predetermined data destruction timetables
- Maintaining the currency of the backup versions of policies and procedures for recreating the network environment, as outlined above, as well as hard copy retention of such should the network be inaccessible
- 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

When 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 health records or designated record sets, amend their records, and receive an accounting of disclosures.

Medical record documentation primarily supports the clinical processes and workflows, and the longitudinal reference to patient care history including recent medications, treatments, or procedures. The documentation captured during the disaster is critical for claims 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, including the lack of users to manually document their workflow
- The physical environment
- Communication limitations
- Reduced workforce availability
- Potential overflow of increased patient admissions beyond census capacity
- Untrained volunteers

The long-term impact of these obstacles may include limited documentation and scattered chart components, which in turn will likely result in problems with future information retrieval efforts. EHR unavailability could be a significant potential patient safety hazard affecting patient care delivery.

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 well-established and practiced BCP should, however, provide a procedure for making decisions under pressure. The need to regularly scheduled tabletop exercises that include a variety of simulated disaster settings will go far to prepare the facility in case of a disaster.

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:

- An Incident Command Center that will be the hub for direction of sustaining operations in the midst of the facility emergency and a central relay-point for coordination of activities
- 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, with paper medical record forms available to replace key EHR functions during the downtime
- 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.3In the midst of a massive and destructive disaster, the hospital may be recognized as a sanctuary location, creating strain on the already impacted facility.

DISASTER PREPARATION

Education and Training

Part of the BCP should include formation of internal incident response teams within the organization. These teams need to be prepared to respond to various situations ranging from internal versus external sources and natural or manmade causes. Education plans and drill processes need to be reviewed at regular intervals to identify changes, gaps, or new scenarios that need to be addressed. 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, documentation integrity, and legal/compliance.

Practicing and Tabletop Exercises

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. When planning exercises or drills ensure all stakeholders are included. These stakeholders might include transportation providers, receiving facilities, and municipalities. Be sure to include various scenarios during the drill.

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”).
- Identify any activities not under normal operations that need to be addressed. During disaster situations privacy and security questions are encountered that staff and volunteers may not be equipped to deal with.
- Share the preliminary plans with the appropriate organizational committee.
- Provide staff with the training and tools necessary to implement the plan. (SeeAppendix B, “Sample Staff Competency List.)
- Test the plan. Retest the plan.
- Fully exercise the plan and make amendments as needed. Evaluation and critiquing exercises 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. Make sure staff expectations are clear.
- 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 theplan
  - 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.
- In the event it is necessary to evacuate, plan for a variety of scenarios including diversion and patients with special needs.
- 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.)

Key Health Record Documents

The manual health record documents that mirror the formats of legal health record documentation in the EHR include:

- Physician Progress Notes
- Physician Orders in triplicate
- Nursing Notes
- Ancillary Services
- Medication Administration Record
- Emergency Department Treatment Record
- Discharge Instructions in duplicate
- Universal Procedure Informed Consent forms
- Authorization to Release Medical Information

Considerations for Staff

During a disaster, staff responsibilities and schedules will likely be altered. It is important to make sure expectations are clearly understood and in the disaster facility role assignments will vary depending upon response needs. Individuals need to know what they are expected to bring for provisions (food, water, linens, and medications) and if child care is provided. Respite areas need to be considered. Alternative facility access and travel restriction are also considerations that must be communicated to staff. Staff with remote access to an EHR system may be called to gather health information to be relayed to care providers in the facility location where the system may be down, particularly as patient and external provider requests for medical information quadruple, specifically for those evacuated from the area.

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 and registered with the incident command center. 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 17 for more information on communication and credentialing professional practitioner volunteers.

Patient Advocacy

Personal Health Records (PHR), Patient Portals, and Health Information Exchanges

Many healthcare providers have implemented 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 health information such as the names of healthcare professionals, medications, allergies, laboratory, and other diagnostic studies and other information that could prove critical during a disaster. Many portals allow patients to upload their own personal health information. When possible, this allows patients to consolidate health information from a variety of sources to one site.

In addition, many healthcare providers have entered into relationships with health information exchanges (HIEs) and record locator services. A health information exchange is a way to share essential health information among participating providers through secure, electronic means. HIM professionals should encourage patients to investigate whether their provider contributes their health information to an exchange. If so, the exchange will have provisions for patient access to information.

With heavy technological reliance, consumers may need to be educated on preparing for a disaster without the use of technology or access to remote sites. Establishing a "personal health record" as a repository for all personal health information has been promoted by AHIMA for many years. Another suggestion is to encourage individuals 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 or purse. Patients with complicated medical histories are strongly encouraged to maintain key records in a sealed waterproof and fireproof container that can easily accessible in a disaster. Copies could also be created to be stored at secondary sites.

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

Assisting Patients with Recovering Their Health Information

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

- The HIM department of the facility may resource a remote process for Release of Medical Information. Instructions and locations can be posted on the facility website, in close proximity to the former location of the facility, or the local public health department.
- If you have access to the Internet, take advantage of the free resources offer by the Office of the National Coordinator (ONC) https://www.healthit.gov/faq/how-can-i-access-my-health-informationmedical-record.
- 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/.
- Call healthcare providers to see if they are in business or have left contact information. If contact can be made, find out the status of personal health records. Ask if they have kept backup copies of health records, lab reports, x-rays, pharmacy, or bills that would be helpful.
- Contact insurance company. It is very likely it can provide documents used in billing (for example, the explanation of benefits statement) to help rebuild a medical record. Medicare enrollees can contact the Centers for Medicaid and Medicare Services online or call 1-800-MEDICARE.
- Contact local pharmacy. Many national pharmacy chains keep a nationwide database with records of prescriptions and can verify names and dosages for the patient and thier healthcare provider, even if the patient has been relocated.
- Contact the 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).
- Investigate if the provider participates in a health information exchange which may have personal health records from providers sorted in arepository.
- Contact any healthcare providers who have been seen on a referral basis (such as home healthcare providers, specialists, surgeons, etc.). These providers may have information sent to them by a referring healthcare provider.
- If there are children, the school district may be able to provide information from the school nurse about a child. If an adult child has attended college, he or she should contact the college for any health information on file.
- Query family to help remember medical history and write down this information.
- Identify what plan you will have if a patient has asked to take their health records as they are going to move away from the area.

HIM OPERATIONS DURING A DISASTER

Communication

Communication Plan

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

Organizations should develop:

- A communication team with plans for each member, including the leadership of health information services.
- An off-site, alternative location for an incident command 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 facilitiesto consolidate the location of disaster victims and their health information.
    - The communication plan should be tested frequently and contact information should be updated. Testing the communication plan via table top exercises and communication broadcasting systems should be performed by an organization's Emergency Preparedness Team.

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

- Maintain an up-to-date list of important contacts (i.e., electronic health record 24/7 contacts, transcription 24/7 contacts, release of information 24/7 contacts) and store it in electronic and paper form.
- Maintain health information staff contact information.
- Mobile telephone cell towers may not be operational, and a list of alternative contact information could assist in quickly identify those who may or may not have service.
- Collaborate with Medical Staff Office to have a current list of all provider contact information.
- Include public health departments (first responders—police, fire and rescue services, Vital Statistics Registrar), state hospital association contacts, local medical societies, tertiary care facilities, 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, although these are not HIPAA secure sites for sharing of medical information.

Planning for media is important to the communication process. The media must have their own space away from the treatment areas with the public relations representative identified by the facility as the facility spokesperson. This facility representative is also the responsible communicator to the emergency management system (EMS) and emergency first responders.

Organizations such as the Red Cross may be on-site. A structured communication plan should be developed and tested to ensure these organizations have the ability to assist disaster victims and their families or significant others if needed.

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 identify triage areas that define how these patients are identified for treatment purposes, but also in regard to questions that may arise from outside requestors (e.g., family members looking for someone). See "HHS Communication in Disasters" section below for further guidance on handling these types of requests.

The atmosphere will likely be chaotic, but every patient needs 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. An example would be using downtime procedures if the EHR system is not able to be used.

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 (handwritten wrist bands, stickers to affix to aperson).
- The Incident Command Center should have a designated area for all supplies needed, including patient labels.
- The use of check boxes on the patient label, colored tags, or colored markers to determine gender, hair color, race, eye color, and age (child, adolescent, adult).
- Descriptions such as "gray-haired female, blue dress, black shoes" may help to later identify the patient.
- Additional measures for correct patient match with existing Master Patient Index, with efforts on minimizing dual medical record number assignment
- A consistent process to identify unknown patients (unable to speak, comatose, etc.) must be in place. An example would be Jane Doe 1, Jane Doe 2.
- Patient identification may be included in patient valuables. Organizations should have a process in place to store patient belongings after the patient has been registered.
- Downtime medical record and registration processes should be tested to ensure that the ability to locate paper forms is accurate. Medical record downtime forms must be routinely updated, in alignment with the form content of the EHR document it mirrors. Downtime documents should be updated as well in the workflow process.

Release of Information

HIPAA regulations allow for disclosure of protected 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 (CE) 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.
- (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 relates 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.

Each state may have unique regulations regarding access to personal health information in a disaster.

Family Members/Patient Companions/Significant Others

Family members, patient companions, and significant others should be located in a designated area apart from the treatment area and the media. A process needs to be in place to inform these individuals of the patient's location and provides a communication mechanism to allow them to make inquiries. Generally, communication to family is done by a communication representative who controls a patient contact list that is received from the patient registration team.

The facility should ensure that staff members who are part of disaster recovery are aware of patient privacy regulations. It is important to document communications made to any individual regarding the patient in the health record or in a patient registry log. As patients are transferred to other treatment facilities, the communication team should be updated, and the medical record should have an updated patient disposition.

All efforts should be made by the Incident Commander to have a mechanism to monitor and control visitors to the organization who do not have a business purpose or related patient at the organization.

Immediate and Short-Term Concerns Checklist

In the event of disaster, immediate concerns require focus, care of immediate needs, and providing 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 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 minimally at orientation and during annual training. Organizations should also conduct departmental and facility-wide drills and 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 devices 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 is to ensure health information is available for the provision of care and operations.

When basic functionality of the EHR system and facility 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:

- Ensuring the confidentiality, integrity, and availability of health information
- Managing business associates within the constraints of a business associate agreement
- Ensuring the physical security of the health information has not been compromised
- 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 reduces confusion when disaster strikes.

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.

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 must 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 hospitals and utilizing EHRs where they may have had little or no previous training. If hospital A transfer 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 patient tracking during a disaster, it follows that discharging patients during a disaster will be problematic since 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 will need to know the location and disposition of patients in order to communicate with numerous individuals asking for this 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 disclose discharge documentation 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 accompanying 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. When developing processes, thought and care should be given to addressing the different types of disasters which require different types of record transfer responses.

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 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.

HHS Communication in Disasters

HIPAA permits the use and disclosure of protected health information (PHI) during disasters to assist in emergency relief efforts and to ensure that patients receive the care that they need. The Health and Human Services (HHS) Secretary will declare a Public Health Emergency which waives sanctions and penalties under certain provisions of HIPAA to facilitate healthcare-related communications in the areas affected by the disaster ("Emergency Waiver"). A link to an example of an Emergency Waiver can be found in the foot note 1.

[1] Waiver or Modification of Requirements Under Section 1135 of the Social Security Act, available at: https://www.phe.gov/emergency/news/healthactions/section1135/Pages/florence-11Sept18.aspx.
The Emergency Waiver also applies to other requirements of the Social Security Act and implementing regulations such as those provisions related to the Medicare Conditions of Participation, EMTALA, health care professional licensure and limitations on physician referral (i.e., Stark). Please refer to the Emergency [2] OCR Issues Guidance to Help Ensure Equal Access to Emergency Services and the Appropriate Sharing of Medical Information During Hurricane Florence, available at: https://www.hhs.gov/about/news/2018/09/13/ocr-issues-guidance-to-help-ensure-equal-access-to emergency-services-medical-information-during-hurricane- florence.html.

In addition, OCR will issue Guidance to assist Covered Entities and Business Associates to facilitate appropriate communications with at-risk populations and to promote equal access to emergency services. Example of OCR Guidance can be found in footnote 2.

The Emergency Waiver

The Emergency Waiver supports covered hospitals providing care to patients and families in distress by temporarily removing the threat of penalties and sanctions under HIPAA.

The Emergency Waiver applies:

- To hospitals, associated physicians, other healthcare practitioners or professionals, healthcare facilities and/or suppliers of healthcare items or services located in the area covered by the public health emergency declaration
- During the period of the public health declaration
- To hospitals that have instituted their emergency response plan/disaster protocol
- For up to 72 hours after the time the emergency response plan/disaster protocol was first implemented

Covered hospitals should document the time and date the emergency response plan/disaster protocol is triggered to ensure the 72-hour timeline can be ascertained.

The Emergency Waiver waives sanctions and penalties against a covered hospital if the hospital does not:

- Obtain the patient's consent before speaking to family members and friends involved in the patient's care
- Comply with requirements related to a patient's ability to "opt out" of the facility directory
- Distribute a Notice of Privacy Practices
- Comply with requests for privacy restrictions
- Comply with requests for confidentialc ommunications

Even where a stricter state law preempts HIPAA and requires authorization prior to disclosing PHI for treatment, pertinent and clinically relevant PHI necessary for treatment may be shared in an emergency without authorization according to federal and state laws.

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. A subcontractor business associate 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 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. This guidance can be found at www.hhs.gov/ocr/index.html.

Other federal and state agencies may also require specific reporting and give waivers during an emergency situation.[3]

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. If PHI has been breached, work with legal counsel to notify the OCR and any accrediting agencies such as the Joint Commission as well as business partners. Contact OCR to obtain clarification on handling records. Inquire if press coverage will satisfy the greater than 500 (affected individuals) provision of the breach notification rule. For more information, visit HHS' guidance on Disclosures in Emergency Situations. For more information https://www.hhs.gov/hipaa/for-professionals/faq/1068/is-hipaa-suspended-during-a-national-or-public-health-emergency/index.html

[3] Appendix E, HHS HIPAA Bulletin: Limited Waiver of HIPAA Sanctions and Penalties During a Declared Emergency."

POST-DISASTER HIM RECOVERY

Inventory and Immediate Documentation Recovery Plans

During the initial post-disaster period with restoration of the EHR system, processes to account for and collect all medical record documentation must be made by HIM staff.

Scanning and image capture volume for hardcopy documents will increase significantly depending on the time the EHR was not available. The entry of scanned documents should be prioritized by current inpatients, those treated and released from the emergency department as well as other outpatient encounters, and inpatients discharged from the facility during the disaster. The prioritization should be based on your routine workflow for scanning and image capture.

Census and patient location resolution will take place first before an EHR system will be allowed to "go live," delayed as much as a day or more, following restoration of the EHR as documentation must be accurately matched to the patient in the correct care delivery location. Patient matching must be audited to ensure proper identification of patient records, minimizing dual medical record number assignment.

Recovery Evaluation and Plans

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

- Evaluating the disaster and the response to the disaster allows the organization to understand what worked well, what needed to be improved upon, and how to identify what might not have previously been included in the disaster recovery plan that should have been.
- Providing feedback to all staff involved in maintaining workflow is also key as they may need to have time to reflect on what occurred, be fatigued, and potentially experience post-traumatic stress symptoms.
- Providing feedback to your vendors (EHR, transcription vendors) is important as they may need to address system failures that they could improve upon (ex. more back up servers to the EHR). If there are costs associated with their recovery of data, that cost should be tracked.
- Sharing the post-disaster and response evaluation with other facilities allows for better preparedness for everyone.
- Assessing resources utilized or expended with the incident and determining the potential for compensation from insurance carriers, FEMA, other designated aid or governmental agencies.

Evaluation and Recovery

- Designate an HIM disaster recovery manager who can be the conduit for the organization's disaster recovery program.
- Develop a recovery work plan with timeframes and work with your HIM vendors (e.g., EHR, transcription, document recovery vendor) to assist in identifying areas that need to be rebuilt, reconfigured, and restored (paper restoration) for full functionality.
- Consider completing a risk assessment or cost benefit analysis to address recovery resources (e.g., is it feasible to recover waterlogged paper records?).
- Paper document destruction should be analyzed by a document recovery company to determine what can be recovered.
- Paper documents that cannot be recovered should be inventoried and a "certification or record of destruction" created so that future requests for information when received will have an inventory of what was destroyed.
- Managing the paper documentation created during the disaster should be included in the disaster recovery plan. This includes determining the timeframe to scan paper into the EMR to ensure the continuity of patient care, the response to requests for information, and the impact on the HIM department to code.

AHIMA

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 (e.g. staffing, supplies, temporary storage), including restoration of systems where backups are available and including estimated time to recreate 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 inaccessibility of 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. When it has been determined that key components of the patient legal health records/designated records are not recoverable, consider creating a "certificate of loss" to be used for future release of information requests:

DECLARATION OF LOST RECORDS

As the authorized Custodian of Records for XXX, I am authorized to certify the status of the patient's health records and declare:

Certification of Available Patient Health Records Copied: The following health records in my custody have been photocopied under my direction and control. To the best of my knowledge, these health records were prepared or compiled by XXX in the course of business and represent the health records available to meet the terms of the request.

Certification of No Records: It is the policy of XXX tomaintainpatienthealth records in accordance with federal and state record retention regulations. In [Month] of [Year], it was determined that a [Describe] incident occurred which resulted in the loss of components of patient health records. In order to mitigate the loss, efforts were made to replicate the data and repopulate the patient health records to the best of the organization's ability. In some cases, replication efforts did not result in exact copies. Despite mitigation efforts portions of patient health records remain unavailable. XXX has determined that lost components of the patient's health records are unrecoverable, and the record is now declared "complete" for filing purposes.

CERTIFICATION OF CUSTODIAN OF RECORDS

I, the undersigned authority, a representative of XXX Health Information Management Department, hereby certify that the record copies attached constitute an accurate duplicate copy of the available patient's original health record originated in the regular course of business and maintained by the organization. The records attached are exact duplicates of the available original health records.

____

[Insert Name and Title of Individual Certifying Copies]

Health Information Management/Medical Record Department

Back to TOC

Debriefing

For compliance, performance should be carefully evaluated alongside the original plan to as certain 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 are 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 informationother 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.

Back to TOC

CONCLUSION

Advancing disaster planning with detailed preparation and practice is an important step for a healthcare organization. To minimize disruption during a time when business and clinical operations may experience their greatest needs, disaster plan deployment and initiation must be organized and systematic. AHIMA's Disaster Planning and Recovery Toolkit is essential to the process as a whole and no steps can be skipped over. Likewise, recovery from a disaster requires a facility-wide team effort. Successful recovery takes working collaboratively with every department within the organization and timely communication in a well-rehearsed, practiced manner to achieve the goal of restoring healthcare operations with minimal disruption to patient care.

By utilizing the Disaster Planning and Recovery Toolkit as guidance to work in tandem with, not replace or supplant the organization's official Disaster Recovery Plan, the health information management professional has a valuable resource designed to bring clarity to a wide variety of procedures and steps that must take place in a predetermined manner in a predefined sequence. Whether the disaster is a result of acts of nature or acts of man, early preparation and practice will help to ensure the organization experiences a successful recovery event and rapid return to normal operations.

Notes

1. Office of the National Coordinator for Health Information Technology, Safety Assurance Factors for EHR Resilience—Contingency Planning, July 2016. https://www.healthit.gov/topic/safety/safer-guides

2. Centers for Medical and Medicaid Services Conditions of Participation

3. 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.

4. 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.

5. Zigmond, Jessica. "Obama Inks Hazard Preparedness Legislation." *Modern Healthcare*, March 13, 2013. http://www.modernhealthcare.com/article/20130313/NEWS/303139943

6. "Health Insurance Portability and Accountability Act of 1996 (HIPAA)." Public Law 104-191. http://www. hhs.gov/ocr/privacy/hipaa/understanding/summary/.

7. 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. https://www.hsdl.org/?abstract&did=767456.

8. Ibid.

9. "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.

10. "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.

11. Office for Civil Rights. FAQ #1067, March 14,2006.

12. Department of Health and Human Services. "Privacy of Individually Identifiable Health Information: Uses and Disclosures—Organizational Requirements." Code of Federal Regulations, 2002. 45 CFR part164, section 504(d)(2)(ii)(D). http://www.gpo.gov/fdsys/pkg/CFR-2007-title45-vol1/pdf/CFR-2007-title45-vol1-part164.pdf.

13. Department of Health and Human Services, Office for Civil Rights. "HIPAA PrivacyRule

14. Compliance Guidance and Enforcement Statement for Activities in Response to Hurricane Katrina."

15. Ibid.

16. Ibid.

References

For more information, please see AHIMA's disaster planning and recovery resources in the

AHIMA Body of Knowledge.

Centers for Disease Control and Prevention. "What Is a Traumatic Event?" June 12, 2003. https://www.cdc.gov/masstrauma/factsheets/public/coping.pdf

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. https://www.cms.gov/Medicare/Provider-Enrollment-and-Certification/SurveyCertEmergPrep/1135-Waivers

CMS Conditions of Participation (Appendix Z, 2018). https://www.cms.gov/medicare/provider-enrollment-and-certification/surveycertemergprep/downloads/advanced-copy-som-appendix-z-ep-igs.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.

Joint Commission Disaster Resources:

- Air Disaster
- Cyber Attack
- Hurricane
- Tornado
- Security/Violence/Active Shooter
- Water Crisis/Industrial Incident
- Winter Storm

Joint Commission Additional Resources:

- Communication/Codes/Alerts
- Exercises and Drills
- General References
- Leadership through Crisis
- Legal/Ethical Issues
- Infection Control/Communicable Diseases
- Vulnerable Populations

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	Weather Event (E.g. Hurricane)	Cyberattack/ compromise of EHR	Manmade Disaster	Other
1	Master patient index (MPI) Patient identification match						
2	Med-Rec Assembly						
3	Deficiency analysis						
4	Coding						
5	Abstracting						
6	Release of Information						
7	Transcription/Dictation						
8	Patient and Chart tracking						
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 health 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 laterdate.

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 health 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 that is stored on another type of storage medium or other storage media.	• MPI will not 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 upsystem • Process is less cumbersome than a totally manual system
Staff members must 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 know show to contact supervisor or manager via text or social media if phone are out for a next ended 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 (e.g., air conditioning,heat)

Account for staff and address immediate needs:

- Use radio and television public-access channels to communicate announcements
- Implement department phone tree (e.g., director calls two people who each call two people) or automated notification system to account for allemployees
- 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), and ensure 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 andusage
- 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)

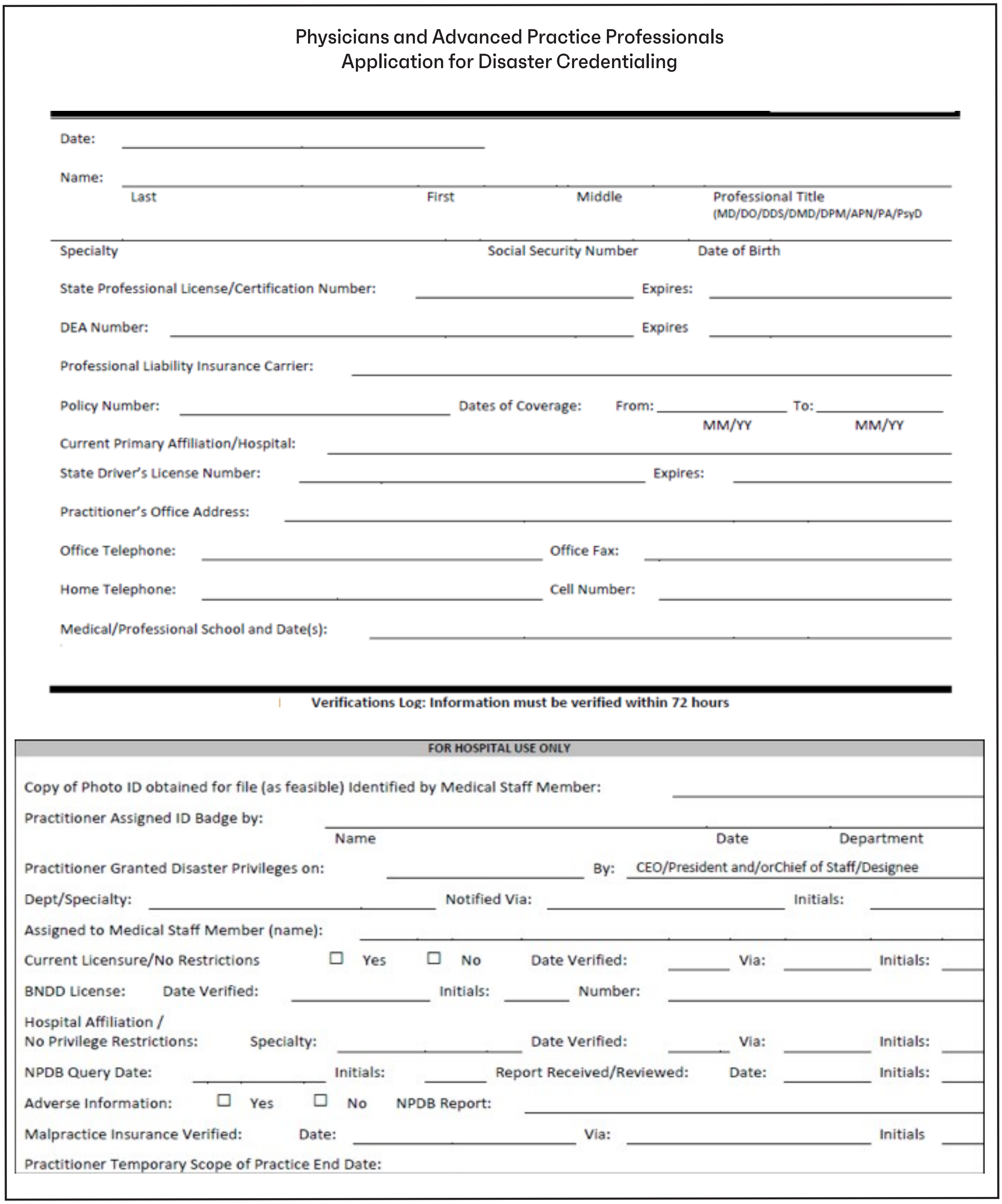
Consult with Human Resources on personnel policies and communicate to staff:

- 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: • Papercharts • 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 ofdocuments: • 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: ______________ To: ______________
MM/YY 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 inpossible 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___________________