Healthcare Business Continuity Management and Disaster Recovery—

No Longer an Afterthought in Today's World

ahia
Assoc. of Healthcare Internal Auditors

Crowe

Authors:

Scott Gerard, CPA
Partner
Crowe LLP

Robert Malarkey,
CISSP, CISA
Crowe LLP

Table of Contents

Increasing Threats in an Already Dynamic Environment 2

Elements of a Business Continuity Management Program 3

When Disaster Strikes: Defining Risk Areas 5

Strategies for Successful Business Continuity Management 9

Making Business Continuity Management an Organizational Priority 11

Conclusion: Internal Audit’s Vital Role 12

Increasing Threats in an Already Dynamic Environment

A healthcare organization's operations and network can be greatly impacted, or even shut down, due to a natural disaster or the harmful actions of bad actors.

The mass shooting in a Chicago hospital in November 2018 was a stark reminder that today's hospitals and health systems face an increasing array of dangers that threaten to disrupt patient care and business operations. Workplace violence in the healthcare industry overall is on the rise, with one recent U.S. Government Accountability Office study reporting healthcare workers at inpatient facilities are five to 12 times more likely to encounter nonfatal violence in the workplace than workers in other industries.[1] Cyberattacks, which can bring down electronic health record (EHR) applications and other vital systems in a matter of seconds, also have become more commonplace.[2]

And, of course, the threat of natural disasters, including hurricanes and fires, is ever present and seems to be increasing, especially in geographically vulnerable areas. A hospital in Paradise, California, may not reopen after sustaining significant damage in the November 2018 Camp Fire.[3] And the effects of 2017's Hurricane Harvey are still very much on the minds of hospital and healthcare facility management in the Houston region as they digest lessons learned and rebuild.[4]

When disaster strikes in an industry as complex as healthcare, the effects can be far-reaching. The consequences of IT failures within a healthcare facility in today's increasingly electronic, data-reliant environment are great, and clinical, operational and financial areas all are at risk should critical systems go down.

With patient lives on the line, the stakes are even higher in healthcare than in other, less complex industries. If hospitals cannot operate their many departments and cannot keep vital IT systems up and running, these organizations could be rendered unable to take care of patients who entrust their lives to them.

All healthcare organizations know the importance of having emergency response plans in place to immediately address disasters, whether natural or man-made. Furthermore, hospitals are required to follow Centers for Medicare & Medicaid Services (CMS), Joint Commission and state authority regulations for emergency preparedness. A primary component of an organization's disaster response is its ability to continue operations as the organization works to recover from a disaster. Business continuity management (BCM) accomplishes this by pre-emptively identifying and establishing plans to continue managing key business functions, processes and their associated IT- or non-IT-related dependencies to minimize the impact of unexpected events on the organization while trying to maintain seamless, uninterrupted operations.

Healthcare internal auditors can bring value to organizational leadership and governance by performing periodic reviews of the organization's BCM and disaster recovery (DR) planning objectives and strategies.

Elements of a Business Continuity Management Program

A well-thought-out BCM program allows an organization to continue functioning during a disaster and, ultimately, to fully recover normal business operations in a timely manner afterward. Through the process of business continuity planning, an organization identifies its main risks, processes and IT systems, and it then creates plans for remediation should a disaster occur.

Though they may intersect with emergency management plans, which are concerned with keeping patients and staff safe from harm during a disaster, business continuity plans (BCPs) are focused on continuing operations when main systems are down. Central elements of a BCM program include:

Business Impact Analysis

A business impact analysis (BIA) is a process to predict the impact on business processes and systems in the event of a disaster in order to develop strategies to recover. Conducting a BIA helps an organization prioritize recovery of each business process and define what those processes need from the following three perspectives:

- **People:** What are the minimum personnel requirements needed to conduct the business process?
- **Technology:** What IT resources (for example, software applications or systems) are required and considered critical to execute that business process?
- **Process:** What non-IT tools, such as patient care instruments and paper charting, are needed to support the process?

To conduct a BIA, business leaders seek input from department owners and stakeholders across the organization to help define and prioritize all critical business functions. A standardized process for establishing ownership and conducting a BIA should exist.

When drafting a BIA, the team doing so should use existing organizational documents and information, including results of the organization's hazard and vulnerability analysis. Other input used for BIA development includes questionnaires (using a standard form) or interviews with experienced staff members within the various departments. Examples of questions to be addressed during a BIA include:

- What are the significant business processes in this department?
- What applications or systems are considered mission critical?
- What resources, including human resources (key players), are required for these business processes to function normally?
- What are the main financial and operational impacts to the department and organization if these business processes cannot be performed?
- What is the recovery time objective for each function? In other words, how long can the department function without doing this business process before it significantly affects the organization? (Number of hours? Days? Weeks?)
- How quickly can these processes be resumed should a downtime event occur?
- What are the department's key dependencies? For example, is there another system that this department's system interfaces with that also should be considered critical?
- Does the department or business unit produce information that is important to another unit? What would the impact be to that department if there is an outage?
- What resources, including personnel, would be required to recover from a major disaster or system outage?

> *A well-thought-out BCM program allows an organization to continue functioning during a disaster and, ultimately, to fully recover normal business operations in a timely manner afterward.*

Output from the BIA should show how important each business process is to supporting the organization overall and help the organization prioritize where it should focus its time, attention and resources in the critical period following a disaster. The input from each business unit is essential to provide a road map for IT in terms of which systems need to be brought back up in what time frame. It's important to note that while the IT function ultimately is responsible for bringing technological systems back up, the business units or departments themselves should own the process of identifying critical systems.

Business Continuity Planning

Using the framework created during the BIA, organizational leadership then can move into creating a BCP. A BCP is a strategic plan that positions an organization's high-risk business processes to be able to function should a disaster occur and major systems shut down.

To develop a business continuity plan, organizational leadership and members of the business continuity team or committee should meet with the crucial process owners within each department to create a plan that can be put into place should a catastrophic event occur. The plan should focus on how each department can minimize impact to the organization and continue operating at an acceptable level during an event. The more thorough the plan, the better (see "Strategies for Successful Business Continuity Management"). The plan should be clear enough for any person to follow, regardless of the individual's everyday role or background.

Disaster Recovery

As a result of conducting a BIA and developing a BCP, the organization should now have a comprehensive list of applications and systems needed to continue operations and a prioritization plan for how quickly the IT department needs to be able to recover those applications and systems. This is known as a disaster recovery plan. While business continuity plans focus primarily on operations, disaster recovery plans largely are an IT endeavor to support operations. When developing DR plans, operational leadership should be involved so the IT department can understand operational processes that need to immediately continue in addition to the supporting applications. As with BCPs, DR plans should be thorough.

Testing

Another crucial component of a BCM program is testing of both business continuity and disaster recovery plans. Teams should conduct tests at least annually using either a tabletop simulation or a full-scale drill. Periodic testing of the plans helps expose incomplete and ineffective procedures that need to be revised or updated to strengthen and refine recovery plans.

When Disaster Strikes: Defining Risk Areas

When critical systems are severely damaged during a disaster, the negative effects on a healthcare organization are multipronged. While different types of disasters—extreme weather incidents, terrorist attacks, ransomware or smaller-scale incidents such as a software malfunction—produce different effects, consideration of risk areas is vital to making sure the organization is prepared to continue operating when crucial systems are down.

Following are examples of some of the biggest risks for healthcare organizations in clinical, operational, finance and IT areas as well as strategies for adequately preparing to continue operations should a disaster occur. The examples can help internal auditors review organizational BCM and DR preparedness and assess the effectiveness of existing plans.

Clinical Risk Areas

Risk:

Clinicians cannot access the EHR and therefore cannot quickly or efficiently treat or diagnose patients. In addition, patients are unable to access their own health information or schedule or change appointments via patient portals.

Risk Prevention Strategies:

- Have a redundant system in place so clinicians can access patient medical history and check for medication allergies; make sure downtime viewers are available for critical applications.
- Have a redundant system or backup (manual) patient portal system in place for patients to access their own medical information or to schedule or amend appointments.
- Develop manual processes for handing off patient information, such as lab information and patient orders, to the lab, the radiology department or other members of the care team.
- Involve medical professionals in BIA and BCP development exercises to make sure critical clinical equipment is prioritized and accounted for; clinicians can provide valuable input to IT about complicated, specialized equipment.

Risk:

Clinicians cannot access electronic systems and must transition to a manual, paper-based system, but newer, less-experienced clinicians are not familiar with how to document or work on paper.

Risk Prevention Strategies:

- Include staff training on paper-based charting in business continuity and DR plans.
- Make paper-based charts and forms readily available throughout the facility and easy to locate.
- Coordinate clinical training (charting) with laboratory staff to cover comprehensive steps for how lab results will be returned and shared.
- Assign a staff member to make sure doctors and nurses are documenting information correctly.

Risk:

Patient handoffs—whether internal or external—are confusing and ineffective due to critical systems being down and communication among clinical departments or with other community healthcare organizations being hindered.

Risk Prevention Strategies:

- As part of overall BCM, have clinical staff conduct an evaluation and inventory of where patient handoffs are likely to occur.
- Include a manual process for documenting internal and external patient transfers in business continuity and DR plans (for example, to document moving patients from ambulatory to an acute care setting internally or externally).
- Designate a staff member to have complete responsibility for patient handoffs when systems are down.
- Make year-round efforts to improve overall coordination among clinical departments, particularly between ambulatory and acute care settings.
- Coordinate with local healthcare facilities and other community organizations to design processes for patient handoffs, and then conduct periodic assessments and tests of those plans.

Operations and Finance Risk Areas

Risk:

Major utilities (for example, electricity and water) are brought down during a disaster, or the facility is damaged and rendered completely unusable.

Risk Prevention Strategies:

- Have a well-equipped command center in place with functioning utilities.
- Prearrange transportation to move patients and staff safely in the event of a disaster. Having learned from Hurricane Katrina, hospitals in the New York City area had arranged for ambulance companies to be on standby should patients need to be evacuated, and they were grateful for that foresight when Hurricane Sandy hit in 2012.[5]
- Schedule periodic inspections of facility backup generators.
- Plan for adequate amounts of fuel and other energy sources to sustain on-site operations in the event that patients and staff are restricted from transport.
- Have contingency plans in place for all major utilities.

Risk:

Critical patient care and facility supplies cannot be delivered or otherwise replenished, and patients cannot be transferred to another facility due to a building lockdown caused by severe weather, such as a blizzard, or other events, such as an earthquake.

Risk Prevention Strategies:

- As part of business continuity planning, staff should assess the organization's inventory of critical supplies.
- Stock enough medicine, medical supplies, food, water, clean linens and other supplies to last for a predetermined amount of time; for many organizations, the goal is the Joint Commission's Emergency Management 96-hour standard or compliance with guidelines from other local, state or federal authorities.
- For supplies typically ordered online, establish an alternative method for placing orders if systems are down.

- Have a plan in place to work with vendors to handle large orders that require advance payment before shipment (for example, orders of expensive pharmaceuticals) if online payments are not possible.
- With infection prevention a top priority, include plans for hiring a third-party service to continue cleaning linens and rooms if these services are not able to be performed in-house for a period of time.
- Have a plan in place for a third-party service to provide ongoing cleaning and sterilization of medical devices.

Risk:

The organization loses revenue because patients have to be turned away (diverted to another facility) because there is no backup (manual) system in place to intake patient health and billing information.

Risk Prevention Strategies:

- Have a process for manually collecting patient billing information, so financial services staff members have complete and correct billing information when they later submit claims.
- Implement a formal manual backup process for physicians to transcribe their notes if the patient accounting system (PAS) is down.
- Consider assigning a staff member sole responsibility to make sure physician notes are properly transcribed and are later captured in the PAS once it is back online.

IT Risk Areas

Risk:

The organization cannot recover vital systems and suffers negative impacts to patient care, reputational damage and financial losses, and it is in breach of federal, local and state regulatory requirements and potentially subject to fines.

Risk Prevention Strategies:

- Have a backup facility in place that is able to bring up the organization's main servers and provide synchronous replication, redundancy and high availability.
- Keep backup copies of software, systems and files in an off-site or alternative location, and make sure they can be brought back up in a timely matter.
- Have redundancies in place on the network between multiple data sites. This gives the organization the ability to use another data site without disruption if one data site goes down.
- Establish contracts for redundant critical technologies such as a redundant internet connection.
- Make sure network capacity is adequate to move large data files between systems if necessary.
- Have an appropriate backup plan or disaster recovery plan for the organization's interface engine (the open link or application that allows other applications within the network to communicate with one another).
- As part of the disaster recovery plan, note whether the organization is able to restore an earlier version of all critical systems.
- When considering backup capabilities and restoration timings, account for changes in complexity and volume of data over time (for example, a considerable increase in the number of patients since the last time business continuity plans were reviewed), and test the ability to migrate large data files from the backup systems to the primary systems.
- If the organization's main building is not accessible (such as during a hazardous materials incident or due to fire or weather-related damage), have controls in place to make sure there is sufficient (remote) network bandwidth and proper equipment to allow staff to work either from home or at a predetermined off-site facility.

Risk:

During downtime, security is reduced, leaving patient health information, payment card information and other sensitive information at risk of being compromised.

> “ *Have a process for manually collecting patient billing information, so financial services staff members have complete and correct billing information when they later submit claims.* ”

Risk Prevention Strategies:

- In the recovered environment, have in place security controls that are the same as or comparable to those in the original environment.
- As part of DR, include a plan for simultaneously recovering the security functions that go with critical systems. For example, if there is a specific firewall in place to protect sensitive patient records, the disaster recovery plan should include that firewall, and it should be brought back up with the EHR.
- Create a plan for destroying any confidential information that was captured on paper during downtime procedures, and decide as an organization how long the paper should be kept in case it needs to be referred to (for example, should the paper be scanned so there is an electronic copy?).

Risk:

As healthcare organizations outsource more and more systems and processes, they are reliant on third parties to maintain critical applications and systems, whether stand-alone applications or those integrated with other in-house applications.

Risk Prevention Strategies:

- Coordinate disaster recovery plans and business continuity plans with all vendors providing third-party applications or hosting critical applications.
- Share updates to BCPs and DR plans, and conduct periodic joint tests with vendors, depending on the criticality of the applications.

Strategies for Successful Business Continuity Management

The following are some of the areas healthcare organizations most commonly overlook when creating business continuity and disaster recovery plans as well as strategies for making those plans more effective.

Revisit business continuity plans and DR plans often. Business continuity and disaster recovery plans are not static documents meant to be created one time and then put away on a shelf. They should be revisited consistently and revised as needed based on changes to departmental processes and software or other infrastructure changes. Commonly overlooked in this area are changes to technology vendors or new IT systems that weren't reflected in the original BC and DR plans. A process should be in place to capture such changes. In addition, BCPs contain vital staff and vendor contact information. As this information changes frequently, plans should be reviewed periodically and updated when contact information changes such as when there is employee turnover. To capture staff information, consider sending an annual or biannual email to employees as a reminder to provide updated contact information to organizational leadership.

Keep business continuity and disaster recovery plans in multiple formats. Unfortunately, some organizations have learned the hard way the consequences of relying on only one format when paper-only plans have burned during a fire or an electronic-only plan was rendered inaccessible due to a system crash or ransomware attack. Keeping BC and DR plans in multiple formats and storing backups off-site are essential practices.

Don't overlook outlier or affiliated facilities. Larger organizations need to consider and include in their BCPs and DR plans any external facilities, such as behavioral health clinics, imaging centers or other free-standing centers belonging to the health system or existing as part of a joint venture with another health system.

Seek input from local authorities and community partners. Working with local community leaders and authorities such as police, fire departments and other healthcare providers is critical when creating BC and DR plans. Local partners can be called on for assistance with emergency response, transportation and even patient care during a disaster affecting the individual facility or one that is widespread throughout a region.

Clearly define roles. Plans should detail who has the authority to declare a disaster and define roles for the organization's disaster recovery team. Depending on the size of the entity, four or five people typically make up the overall disaster recovery team, covering areas such as communications and media relations, resources and supplies and workforce. Each of these people will lead a team of individuals who can take action during an event and make sure disaster recovery and business continuity plans are executed. The IT department typically has a separate disaster recovery team that includes a point person who determines budget and resource allocation and maintains contact with vendors.

Identify in advance any temporary staffing or vendors that might be needed during a disaster. Business continuity plans should include contact information for additional staff required. Consider assigning a staff member the role of managing temporary staff during a downtime or disaster event.

Keep up with training. Training staff in BCM and disaster recovery may seem like one more to-do item in an increasingly busy work environment; however, in the midst of a disaster is not the time to learn about the organization's business continuity and disaster recovery plans. Organizational leadership should require training at regular intervals—at least annually—and be sure to include plans for training new employees during the onboarding process.

Consider having a third-party consultant review the organization's plans. An outside perspective can help organizational leadership challenge existing business continuity and disaster recovery plans and note areas for improvement. The bird's-eye view can be valuable, especially for organizations that have been experiencing change in management, operations or IT systems and for those that have been using similar plans for many years.

Test, test and test some more. Testing the overall business continuity plan, including disaster recovery, is paramount to validating effectiveness in the event of a disaster. Testing should be conducted at least annually, and many organizations benefit from more frequent testing, depending on the size and scope of the facilities involved. Some organizations find tabletop exercises to be helpful. During these events, key stakeholders from departments across the organization walk through various disaster scenarios featuring loss of IT systems. These tabletop exercises typically include "injects" in which twists to the scenario are added to help participants probe what they might do should scenario X, Y or Z happen.

Some organizations' IT departments periodically conduct downtime exercises during which they take down a main system, such as the organization's EHR, and then try to restore it from backup within a specified time frame. And many organizations already practice full-scale disaster simulation drills, such as those required by CMS.[6]

Finally, whether conducting a full-scale, communitywide drill or a biweekly IT downtime simulation, organizations should have a formal procedure to capture and address lessons learned from tests performed. Also, lessons learned from other organizations that could experience the same or even different types of disasters should be evaluated, wherever possible, so additional perspectives can be considered. This will help organizations be even better prepared for various disaster scenarios. Just as facilities learn valuable lessons after the fact when an actual event occurs, indispensable insights can be gleaned from drills and other simulation exercises, with the information then being used to revise and update BC and DR plans.

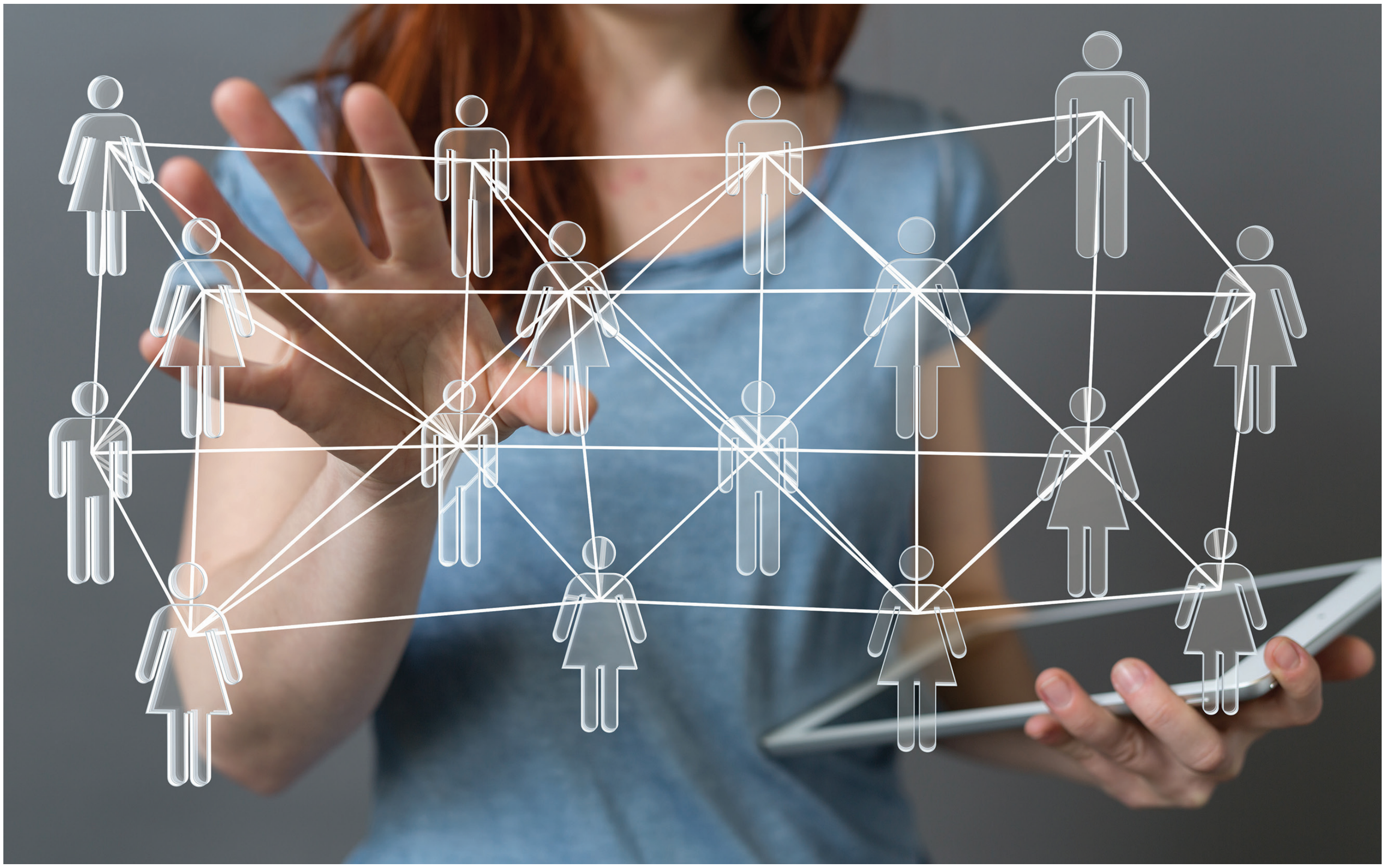
Making Business Continuity Management an Organizational Priority

For business continuity management efforts to be most successful, they need to be among an organization's top priorities. This can be an understandably tall order for many healthcare organizations in an era marked by stretched financial and human resources.

As with many organization-wide initiatives, business continuity management requires a commitment of support from organizational leadership, including the board. The following strategies for making business continuity management more of an organizational priority should be considered:

- Include discussion about BCM on the board's and C-suite's meeting agendas. Help establish or enhance tone at the top.
- Appoint a member of the leadership team to own business continuity management, including responsibility for updating plans at least annually; depending on organizational size, this may be the individual's sole job.
- Include discussion about BCM and DR plans in daily or weekly departmental meetings.
- Regularly communicate information about BC or DR plans with staff members to increase awareness.
- Consider the impact to BC and DR plans when implementing new IT systems, moving applications to a hosted environment or making significant changes to operating departments.
- Consider including a BCM-related objective on senior leaders' annual reviews.

> *As with many organization-wide initiatives, business continuity management requires a commitment of support from organizational leadership, including the board.*



Conclusion: Internal Audit's Vital Role

In a complex and continuously evolving healthcare industry that faces more threats than even just a decade ago, today's hospitals and health systems need to be more prepared than ever to continue operations should a disaster occur. Healthcare internal auditors play a critical role in assessing whether an organization is meeting business continuity management objectives. These objectives include formulating thorough, standardized business continuity and disaster recovery plans—with considerations for the essential processes, personnel and resources, including external partners, needed to navigate an event—and overseeing testing and follow-up for all plans.

Working with organizational senior leadership, healthcare internal auditors can help make sure business continuity management is effective so the organization is ready to serve patients even when unexpected events occur, disasters strike or major systems are unavailable.

Endnotes:

[1] "Lawmakers Seek OSHA Standard on Workplace Violence Prevention in Health Care," Safety+Health, March 14, 2018, https://www.safetyandhealthmagazine.com/articles/16776-lawmakers-seek-osha-standard-on-workplace-violence-prevention-in-health-care

[2] Aziza Kasumov, "Cyberattacks on Health-Care Providers Are Up in Recent Months," Bloomberg, July 17, 2018, https://www.bloomberg.com/news/articles/2018-07-17/cyberattacks-on-health-care-providers-are-up-in-recent-months

[3] Risa Johnson, "Feather River Hospital: 'We Don't Know If We Will Reopen' After Camp Fire," Chico Enterprise-Record, Nov. 28, 2018, https://www.chicoer.com/2018/11/28/feather-river-hospital-we-dont-know-if-we-will-reopen-after-camp-fire/

[4] Sheri Fink and Alan Blinder, "Houston's Hospitals Treat Storm Victims and Become Victims Themselves," The New York Times, Aug. 28, 2017, https://www.nytimes.com/2017/08/28/us/hurricane-harvey-houston-hospitals-rescue.html?smid=tw-nytimes&smtyp=cur

[5] John Palmer, "Five Lessons That Have Made Hospitals Better Prepared Since Hurricanes Katrina and Sandy," Patient Safety & Quality Healthcare, Dec. 6, 2017, https://www.psqh.com/news/five-lessons-made-hospitals-better-prepared-since-hurricanes-katrina-sandy/

[6] Centers for Medicare & Medicaid Services, "Emergency Preparedness Rule," https://www.cms.gov/Medicare/Provider-Enrollment-and-Certification/SurveyCertEmergPrep/Emergency-Prep-Rule.html

ABOUT AHIA

The Association of Healthcare Internal Auditors (AHIA) is a network of experienced healthcare internal auditing professionals who come together to share tools, knowledge, and insight on how to assess and evaluate risk within a complex and dynamic healthcare environment. AHIA is an advocate for the profession, continuing to elevate and champion the strategic importance of healthcare internal auditors with executive management and the Board. If you have a stake in healthcare governance, risk management and internal controls, AHIA is your one-stop resource. Explore our website for more information. If you are not a member, please join our network, www.ahia.org. AHIA white papers provide healthcare internal audit practitioners with non-mandatory professional guidance on important topics. By providing healthcare specific information and education, white papers can help practitioners evaluate risks, develop priorities, and design audit approaches. It is meant to help readers understand an issue, solve a problem, or make a decision. AHIA welcomes papers aimed at beginner to expert level practitioners. This includes original content clearly related to healthcare internal auditing that does not promote commercial products or services. **Interested? Contact a member of the AHIA White Paper Subcommittee.**

SUBCOMMITTEE:

Alan Henton, White Paper Chair
alan.p.henton@vumc.org

Mark Eddy
mark.eddy@hcahealthcare.com

Linda Greer
tlbmc@cox.net

Debi Weatherford
debi.weatherford@piedmont.org

Laura L. Sak-Castellano
Laura.Sak-Castellano@advocatehealth.com

Deborah Pazourek, AHIA Board Liaison
Deborah.L.Pazourek@medstar.net

ahia
Assoc. of Healthcare Internal Auditors

Crowe