Preparing the Way

Disaster Readiness and Business Continuity Planning
Our Commitment to Recovery and Healing

So many tragic events occurred during 2017 in the United States. Destructive hurricanes ravaged the southern Continental United States (U.S.), Puerto Rico, and the Virgin Islands. Devastating fires damaged parts of California. Tragic mass casualty events such as the shootings in Las Vegas left communities shaken and families in need. The consequences have been profound and recovery efforts are ongoing.

Disasters come in all shapes and sizes. Each type of disaster may bring with it unique circumstances that require unique responses. Disasters may require relocation of health care facilities, new requirements for vaccinations, loss of medicines or medical equipment, mass casualty or advanced trauma care, and expanded mental health counseling and support resources following the incident.

Health insurance providers are uniquely situated in the health care ecosystem. We are a critical link to helping consumers access and use health care services leading up to, during, and in the aftermath of these disruptive events. We are there for those who suffer physical injuries and need emergency care. We offer pathways to long-term rehabilitation and emotional support. We are committed to working together for their recovery.

Since 2005, AHIP has met regularly with members of our Emergency Preparedness Work Group on national emergencies and disasters. We also convene ad hoc conference calls and events with our Chief Medical Officers for public health emergencies and updates. In addition, we have frequent communications with our federal partners to prepare for and respond to the aftermath of disasters.

While natural and manmade threats remain, new and changing threats like cybersecurity, terrorist events, and mass casualty shootings have also emerged as additional areas of concerns. At the same time, advances in technology and digital communication tools have transformed the landscape of emergency preparedness and response.

As a part of our enduring commitment to ensure patients receive the care that they need, health insurance providers continue to refine emergency protocols to best serve their members, employees, partners, and communities. Our goal is that this issue brief can serve as a resource for health insurance providers, offering best practices for emergency preparedness and business continuity.

Marilyn Tavenner
President and CEO, AHIP
**Definition of Disaster**

A disaster is any natural or human-created event that has a widespread and enduring impact on a community. These events may hinder members’ or beneficiaries’ ability to get care and support. Such events could result in:

- Disruption of crucial community resources, such as health care and emergency services; power and communication systems including telephone and internet; mail delivery; access to food, water, or housing; or the ability to travel freely.

- Significant interference with key business functions or processes of the health insurance plan, such as a crippling cyberattack.

- Evacuation or relocation of large numbers of individuals away from their usual health care providers or delivery networks.

- Stress on health care providers, delivery networks, and delivery systems beyond capacity.

**Preparing for a Disaster**

There are actions that health insurance providers can take to prepare for and respond to a disaster.

- **PLANNING:** Develop and maintain an enterprise-wide process, including a comprehensive and detailed business continuity plan. This plan should be flexible enough to adapt to changing circumstances.

- **COMMUNICATIONS:** Inform critical audiences, including employees, consumers, customers, providers, business partners, media, and government agencies about actions to be taken before, during, and after a disaster, where to access additional information, and how to get questions answered (e.g., toll-free emergency hotline, online).

- **COORDINATION:** Work together with customers, providers, business partners, media, government agencies, and other stakeholders to improve community-wide preparedness.

**State of Emergency Preparedness for U.S. Health Insurance Providers**

In 2015, the *American Journal of Managed Care* published the results from a survey of AHIP members about emergency preparedness¹. This included topics such as infrastructure, adaptability, and connectedness. The data represented the first national perspective for health insurance plans’ emergency preparedness. The respondents represented more than 190 million members and 81 percent of total health insurance plan enrollment in the United States. Major findings include:

- **All respondents** had emergency plans in place for business continuity in the event of a disaster², and **85 percent** had infrastructure to support emergency teams.

- **More than 95 percent** of respondents indicated that a federal or state emergency declaration would automatically trigger an internal review of policies and benefits.

- **85 percent** had protocols to extend claim filing time.

- **71 percent** could temporarily suspend prior authorization rules.

Emergencies require special attention for patients with specific health care needs. Nearly
all respondents reported that they can monitor patient needs and prescription medications through claims information. More than a third of plans had capabilities to monitor and support patients with potentially urgent health care needs—e.g., those dependent on durable medical equipment (34 percent), prescription drugs such as insulin and methadone (46 percent), and home health care (35 percent).

The survey also revealed opportunities for improvement. While 82 percent of plans participated in internal preparedness drills, fewer than 30 percent participated in drills with external stakeholders.

Building a Disaster Plan

Planning is at the heart of response readiness. It allows entities to consider the possible impact of a catastrophic event. It is widely accepted that planning for disasters should be directed at all hazards, rather than at any one type of hazard. Most disasters—earthquakes; hurricanes; floods; fires; chemical, biological, and radiological/nuclear incidents; shootings and mass casualty events; and infectious disease outbreaks—can be addressed in a single plan. There are some instances, due to the special nature of the threat, where a specific module can complement an overall business continuity plan.

The planning process should address the need to restore the health insurance provider’s business and administrative operations, and the potential long-term effects that may result from a major disaster. This would include, but not be limited to, issues such as long-term disruption to communication networks, as well as the impact of large-scale evacuations—which may include a significant percentage of the plan’s workforce.

Key Steps for Disaster Planning

1. Leverage executive leadership
2. Create planning and response teams
3. Assess and prepare for potential risks
4. Develop the plan
5. Communicate updates to relevant stakeholders
6. Train the workforce and test the plan
Preparing the Way

1. Leverage executive leadership

Executive leadership is essential. Often, emergency response plans require coordination across several different departments. Human resources, customer service, central command call centers, and internal/external communications can all be affected (e.g., increased call volumes from consumers, inquiries from other stakeholders, etc.). Establishment of an executive oversight committee demonstrates a clear commitment to emergency preparation.

2. Create planning and response teams

Some insurance providers have designated employees with specific responsibilities to prepare an enterprise-wide contingency plan. This same team would implement the plan when a disaster strikes. After the planning process, everyone involved would have a clear understanding of their responsibilities, with established lines of authority.

The planning process could include not only the health insurance providers’ workforce, but other stakeholders—such as hospitals, physicians, and other health care providers, consumers, public health officials, and vendors—that would be critical to continuing services in the event of a disaster.

Teams can address areas such as human resources policies, legal and regulatory issues, and outreach to community leaders, consumers, providers, government agencies, businesses, and social services organizations. To maximize effectiveness, each of the teams—which may include damage assessment, information technology recovery, business resumption, and administrative support workgroups—could be equipped with the tools and authority to make decisions, communicate with stakeholders, troubleshoot, and improvise, when necessary.

Each disaster comes with a unique set of circumstances that requires a significant amount of immediate decision-making outside the normal corporate decision hierarchy. Encouraging employees to creatively and quickly problem solve or "think on their feet" when necessary is critical. For example, many health insurance plans affected by Hurricanes Harvey, Irma, and Maria changed their business operations rapidly because of the widespread displacement of health care providers across the impacted regions in addition to loss of critical infrastructures such as electricity, roads, and other vital services.

3. Assess and Prepare for Potential Risks

While all-hazards planning implies a focus on all types of disasters and business disruptions, teams could also consider developing a hierarchy of threats or hazards, an estimation of exposure, and a prioritization of actions, resources, and responses to address them.

Many health insurance providers design their disaster response plans considering critical business functions they routinely provide for members, customers, providers, vendors, and business partners. These functions can be categorized based on how quickly they should be restored:

- **Category 1**: Business functions that cannot be compromised and require “real-time” continuity.
- **Category 2**: Business functions that must be restored within 24 hours.
- **Category 3**: Business functions that must be operational within 48 hours.
- **Category 4**: Business functions that must be operational within 72 hours or later.
4. Develop the Plan

The completion of the risk assessment and prioritization stage allows planning teams to identify those key resources and support that will be needed.

- Identify those external systems and business partners which may be affected (e.g., members, customers, health care provider networks, business service providers, pharmacies, vendors, and government agencies).

- Create an enterprise-wide business resumption strategy which goes beyond information technology to include critical business systems such as communication networks and consumer call centers.

- Require each business unit to establish a disaster response plan that integrates with the enterprise-wide strategy.

- Establish a process and system to communicate with employees, members, and the public. Communication tools include updated webpages with need-to-know information for members, mass e-mail distributions, press releases and other media resources, and other digital platforms (including handheld devices). The system should also outline non-technical tools that can be used to communicate with members in the event of an emergency that limits access to electronics.

- Provide employees with a toll-free telephone number and/or web platform in the case of an emergency. Consider printing this number and/or web address on employee identification badges.

- Pre-position supplies such as generators and communication devices (perhaps including satellite phones and e-mail handheld devices) should power or communication networks be compromised.

- Develop a plan to establish alternate office locations to transfer workers in situations where an emergency may make the business office unusable.

Central Command Centers

A common strategy is to create or identify a site to serve as a central command center to coordinate and implement disaster plans. Emergency response teams could be assigned to a command center and policies can define responsibilities and overall command authority.

Key employees may be identified for each functional area and a temporary work location could be designated. Depending on how far employees must travel to get to recovery sites or other geographic locations, health insurance providers might consider providing back-up transportation. Back-up personnel could be identified in case emergency response team members are not available.

Command center personnel would have access to disaster plans, reference manuals, resource directories, information management systems, equipment, and supplies as well as emergency power and redundant communication systems to ensure capability for gathering and disseminating critical information. These resources should be available through a secured online portal, as well as through hard copy materials.

In some cases, local or regional command centers, or other secondary centers and bases, may be needed depending on the size of the health insurance provider and the types of business operations which could be affected by a disaster.
5. Communicate updates to relevant stakeholders

**Internal Communications**
Getting the word out to employees and other workforce members is essential to an effective response. Health insurance providers may explore several communication networks—including digital platforms, toll-free telephone numbers, satellite phones, and internet/website resources—to communicate with staff. Expect that in major disasters or storms, telephone lines and cellular towers can function intermittently or fail.

Employees need to have a clear understanding of where to go for information. Many health insurance plans include a toll-free “emergency hotline” on the back of employee identification badges. Employees may be asked to call their employers or check-in on a web platform to report if he/she has been affected by the disaster and to allow the employer to determine whether the employee is available to assist with recovery efforts. Longer-term communication strategies may also be needed in certain situations. Providing the means for certain employees to work remotely may be a particularly successful strategy during a pandemic emergency.

**External communications**
To minimize business interruption, communication with external stakeholders (e.g., members, consumers, providers, vendors, regulators, public health officials, the news media, and others) should be carefully planned, and be flexible to respond to the situation. Health insurance providers may establish a process for maintaining open lines of communication with state and federal regulators, public safety and health officials, business partners, and health care provider networks until normal operations resume. Plans can also make homepage updates where disaster protocols may be quickly accessed through a webpage banner alert.

Health insurance providers can establish a process for members, health care providers, plan sponsors, and vendors to report their status after situations where there is large-scale disruption of community services or damage to homes, businesses, and infrastructure. Local and state medical societies and hospital associations may be partners in identifying which providers are operational after a disaster occurs. Key audiences (members, providers, vendors) can be updated on the company’s disaster response activities through communication venues such as conference calls, newsletters, meetings, and websites.

Depending on the severity and duration of the disaster, health insurance providers may review policies relating to:

**A temporary suspension of rules for:**
- Prior medical authorizations;
- Pre-certifications;
- Reimbursement restrictions;
- Utilization management review of in-hospital cases; and
- Pharmacy re-fill limitations and co-payments.

**Temporary deferrals for:**
- Rate increases;
- Premium payments;
- Cancellations; and
- Enrollment.

**Other possible options include temporarily:**
- Providing access to critical prescriptions for members—including shipping prescriptions to members at alternative addresses;
- Applying cost-sharing requirements to enrollees for all medical services as if they were received from “in-network” health care providers; and
Preparing the Way

• Leveraging electronic records to assist consumers and pharmacists with re-tracing an individual’s prescriptions that may now be lost or inaccessible, or where prescription records have been destroyed.

Health insurance providers should train customer service, provider service, and nurse assistance staff on emergency-triggered rule modifications.

Reaching Out to Business Customers
In the event of a disaster, it is essential to communicate regularly with business customers to assess their needs, inform them of the health plan’s current operational status and the timeline of response activities, and collaborate to improve recovery. Personal outreach by plan representatives should be complemented with website and telephonic-based information flow.

Reaching Out to Providers
Health insurer providers may develop a contingency plan with state provider organizations such as hospital associations and medical societies to prepare for an event. Both are good resources for determining whether medical services are available in an area and for disseminating information to their hospital and physician members.

Contingency planning can inform providers of temporary exceptions to normal procedures (e.g., utilization review, pre-authorization requirements, prescription drug refill limits). Health insurance providers can provide a designated plan contact for providers to use to seek answers to their questions and resolve problems.

Reaching Out to Vendors
Vendors and suppliers have their own disaster response plans to provide for continuity of services to their customers. Health insurance providers negotiate provisions in contracts with vendors to address business continuity. These partners can support key functions (e.g., claims processing, provision of medical supplies) in case the health insurance provider’s primary or secondary recovery fails. Plans and vendors should plan for how best to pre-position goods and services when a disaster disrupts normal supply outlets.

Reaching Out to Government Officials
Collaboration between health insurance providers and local, state and federal officials prepares everyone for future disasters. Actions that may be taken include the following:

• Develop contingency plans: Share contingency plans and contact information with emergency officials. Inform regulatory agencies on how business operations can be affected and engage them in dialogues on appropriate agency and health insurance plan responses. Develop a communications process with regulatory agencies and public health officials that can be implemented when events occur.

• Develop disaster response option guidelines: Develop guidelines for specific actions by health insurance plans to assist the public in maintaining access to health care and health insurance coverage depending on the nature, scope, and extent of the disaster event.

• Develop emergency contact lists: Create and update, as necessary, lists of key health insurance plan personnel and provide those lists to local, state, and federal emergency officials, and the state department of insurance.

• Identify emergency agencies which could be involved in relief efforts: Create and update, on a regular basis as necessary, lists of contact persons, phone numbers,
Preparing the Way

and addresses of local, state, and federal emergency personnel.

- Participate in federal or state agency emergency update calls, as appropriate: Often, state or federal offices may hold regular update calls across stakeholder groups. These conference calls serve as a useful opportunity to make groups aware of on-the-ground activities and flag potential issues.

- Stay up-to-date on federal and state emergency warnings, declarations, and bulletins; this includes keeping informed of weather patterns and changes, road closures, and/or evacuations.

- Collaborate with agencies after a disaster: Once the federal or state government declares an emergency, it is important to continue to work closely with regulatory and emergency agencies to respond to the needs of customers and the public. For example, health crises can evolve after an event (e.g., vaccination needs, disease outbreaks following floods).

6. Train the Workforce and Test the Plan

Health insurance providers should train their workforce to ensure that every employee understands their responsibilities in the event of an emergency. New staff orientation should include information regarding these details as well.

Many health insurance providers regularly test their business continuity plans for effectiveness, flexibility, and compliance with applicable state and federal requirements. These plans should be periodically updated plans for new threats. Testing can range from simple "table top" exercises to full-scale deployment of workforce and operational systems. Disaster recovery "dry-runs" may include both internal operations and external audiences (e.g., providers, vendors, and government agencies).

Personnel that oversee business response and continuity should evaluate the performance of the plan after each drill. The evaluation might include the following questions:

- Is the workforce familiar with their duties and responsibilities in responding to a disaster?

- Do they have information about threats, hazards, and protective actions?

- Are employees prepared to follow emergency response and shutdown procedures?

- Is the workforce familiar with evacuation, shelter, and accountability procedures, as well as location and use of common emergency equipment?

- Are the disaster response operations of vendors, suppliers, and providers integrated with the enterprise contingency plan?

- Are communication systems available and configured to inform the workforce, business partners, and consumers?

- Are planning and response processes fully integrated with local and state emergency response efforts?

- Is the contingency plan sufficiently flexible to respond to different types of disasters?

Contingency planning is an on-going process. It is important to add, modify, or remove plan components as needed. Significant changes in business operations, markets served, facilities, information technology systems, and methods of communications may trigger a review audit with corresponding adjustments to the plan.
Conclusion

Preparing for a catastrophe requires planning, teamwork, and collaboration. Gathering a response team and preparing a contingency plan are the first steps in a long process to responding to a disaster. Understanding the company's vulnerabilities and minimizing risk are an integral part of the planning process.

Once a disaster strikes, health insurance providers focus their efforts on the timely resumption of vital business operations. A plan’s success depends on the degree of collaboration with consumers, employees, vendors, health care providers, government agencies, and other community organizations to provide a unified disaster response. Equally important are ongoing communications between those entities accountable for responding to a catastrophic event so organizations and public officials are not working at cross purposes. Above all, the approach taken should be flexible to meet different types of disasters and changing needs throughout the course of a disaster.

These events can have long lasting impacts on communities. Health insurance providers stand ready to support their members and these communities in preparation, execution, and recovery efforts.

Endnotes


2 The Health Insurance Portability and Accountability Act Privacy and Security regulations serve as a foundation for contingency planning for health care entities. The regulations helped focus health sector resources and consistency for emergency preparedness and responses
Case Study – Responding to Severe Weather

The unparalleled hurricane season of 2017 saw several storm systems make landfall within days of each other. With Hurricanes Harvey, Irma, and Maria hitting the Southeast in quick succession, health insurance providers quickly reacted to changing circumstances across different states. In the days and hours leading up to the storms, health plans circulated digital communications, established 24/7 call center lines, and updated their digital platforms so members could quickly access their health information as they made their own plans for the storms. Call center lines remained open throughout the duration of the storm.

Following the storms, plans conducted check-ins to evaluate member and employee health and welfare. Often, outreach was conducted via telephone and email. Across the region, plans established crisis intervention hotlines, accessible to all residents within the storm’s path, to provide behavioral counseling and emotional support to members, families, and individuals in the community.

Further, health insurance providers leveraged telehealth capabilities to connect patients to care and services. Several health plans, hospitals, and telehealth firms offered video-based consultations for individuals impacted by the storms. Further supporting these efforts were state-level actions directed at expanding access to telehealth services. For example, in Texas, Gov. Greg Abbot temporarily suspended physician licensure requirements so that health care providers “in good standing” in another state could assist with Hurricane Harvey disaster response operations.

Case Study: Mass Casualty Events

Mass casualty events leave communities shaken and families in need. The consequences of these disasters can be profound. That’s why health insurance providers are committed to helping everyone recover, rebuild, and restore their futures. Insurance providers are there for every victim, from those who suffer physical injuries and need immediate emergency care, to those who need long-term rehabilitation and support, to those who need counseling and emotional care, including 24/7 hotline support to expanded access to licensed therapists and psychologists.

Following 2017’s mass shooting in Las Vegas, health plans worked closely with community care providers to coordinate care for their patients, to help ensure easy access for ongoing medical needs, and to address potential out-of-network expenses. Health plans serving the Las Vegas community also launched 24/7 crisis hotlines for residents impacted by the shooting.

Case Study: Cybersecurity

As individuals, businesses, and government organizations increasingly engage across digital platforms, the continuous threat of cyberattacks poses serious challenges to consumers’ privacy, national security, and the broader U.S. economy. The health care industry is not immune to cybersecurity risks. In recent years, cyber threats, ransomware attacks, malware, phishing schemes,
Preparing the Way

hackers, threats from hostile state actors, and other malicious threats have continued to impact the health care sector, non-health business sectors, public agencies and organizations, and individuals themselves.

Outside of risks to traditional claims databases, the digitization of health care has produced additional cyber vulnerabilities across the health care system. Everything from a pacemaker and X-ray machine, to a patient’s mobile fitness app and a large-scale health database are potentially at risk.

Health insurance providers are prioritizing their readiness to counter and defend against these attacks through targeted prevention and detection operations as well as consumer protection and support efforts. Organizational size, business software, internal and external resources, types of electronic data, and a host of additional factors cause health insurance plans to heavily invest in tools and support to prevent data breaches and cyber-attacks. Emergency managers should plan and prepare for cyberattacks the same way they prepare for natural disaster events such as hurricanes and tornadoes.

Key activities include:

- Inventory data types, transmission methods, “data at rest” storage systems and databases that house, move, store, or affect electronic data.
- Staying up-to-date on hardware and software alerts, “patches,” system updates, and industry alerts and events.
- Developing information and notices for consumers to understand how their data will be used, disclosed, and protected.
- Training executives, staff, vendors, and contractors.
- Keeping aware of public announcements related to cybercrimes, threats, and ongoing law enforcement activities.
- Collaborating with public and private entities about trends and schemes, and resulting best practices to defend against them,
- Remaining vigilant over data security policies and procedures with a keen eye toward how human errors can unintentionally or intentionally undermine a system infrastructure.