E Emergency Response and Disaster Recovery Plan

REQUIREMENT: RFP Section 60.7 E
E. Emergency Response and Disaster Recovery Plan
Describe the Vendor's proposed emergency response and disaster recovery plan, including a summary of how the plan addresses the following areas:
1. Essential operational functions and responsible staff members;
2. Plans to ensure critical functions and continuity of services to Providers and Enrollees will be met;
3. Staff training;
4. Contingency plans for covering essential operational functions in the event key staff are incapacitated or the primary workplace is unavailable;
5. Approach to maintaining data security during an event;
6. Communication methods with staff, Subcontractors, other key suppliers, and the Department when normal systems are unavailable; and
7. Testing plan.

We will leverage the extensive experience and best practices of our affiliated health plans to develop a proven emergency management plan tailored for Kentucky Medicaid using modern security and highly trained staff to respond to a variety of incidents.

An emergency response and business continuity plan must provide the guidance necessary to maintain continuity of operations. The ability to provide immediate support to our Enrollees, our providers, Commonwealth staff, and our employees managing challenges is of paramount importance.

Our approach to disaster recovery and business continuity, our Business Continuity Management (BCM) program, is comprehensive and captures mission-critical business processes, information systems, and associated infrastructure. The program consists of emergency management, incident management, business continuity (BC), and IT disaster recovery (DR) plans and provisions.

- Comprehensive set of emergency and business continuity procedures proven effective during emergencies
- History of successful service delivery during huricanes, floods, pandemics, and terror attacks
- Modern, cloud-based data center solution with enhanced security to protect data
- Industry-leading approach using best practices developed by DRI International, ISO 22301, and NIST, as well as our own experience

Our organization's emergency response capabilities have been put to the test on more than one occasion and in various types of emergencies or disasters, ranging from localized power outages to major regional disasters. We have successfully faced the challenges of hurricanes, including Ike, Sandy, Harvey, Matthew, Irma and Maria; the H1N1 pandemic; the 2015 San Bernardino terrorist attack; major flooding in South Carolina and Louisiana; and the 2016 water crisis in Flint, Michigan. We understand that high winds, tornadoes, flooding, and severe winter storms are very real threats to the Commonwealth and its citizens. We are prepared to leverage our local knowledge and the extensive experience of our affiliated health plans to ensure continued services and support of Kentucky Medicaid program operations.

Furthermore, our **modern, cloud-based data center solution** has enhanced security to protect data, including tools for threat intelligence, multi-factor authorization, and threat analytics, and provides a scalable storage and backup solution allowing for an application to be recovered in minutes versus hours.

These tools are used in real time to quickly identify threats and suspicious activity on the network. Placing data centers in different locales improves availability, enables effective load balancing, guards against local broadcast storms and potential configuration problems, and provides a truly redundant operating environment.

Bringing Best Practices for Collaboration Across the Commonwealth. At our organization, facilitating exceptional care for members covered by government contracts like the Kentucky Medicaid program is our only business, not just a line of business. As such, our emergency response and business continuity plans were developed specifically to meet the needs of our clients and their most vulnerable populations. Molina is committed to partnering with the Commonwealth, fellow MCOs, and providers to share our best practices and to ensure continuity of care for Enrollees no matter the incident.

A best practice culled from our experience nationwide is collaborating with fellow MCOs in preparation for and during an incident. For example, in collaboration with our affiliate health plan in Puerto Rico during the catastrophic hurricanes of 2017, members of our Incident Management team worked directly with fellow MCOs to ship supplies to the island, store the supplies when they arrived, and distribute the supplies to members and employees. We look forward to bringing our best practice of collaboration and communication with fellow MCOs to the Commonwealth.

In preparation for a disaster, we will facilitate webinars and an in-person symposium with fellow MCOs, Department staff, and industry subject matter experts to educate, train, coordinate, and plan as a cohesive front for any disaster that could affect Kentucky and its Medicaid population. ***This proposed format also will support cybersecurity and privacy.***

Using our proven incident approach and experience, along with our highly skilled and trained teams, we will ensure our plan is tailored to mitigate incidents that may impact the Commonwealth. ***The remainder of this section describes our proposed emergency response and disaster recovery plan.*** We provide a summary of how the plan addresses each of the requirements within RFP Section E, Emergency Response and Disaster Recovery Plan. In addition, within Attachments to Section D, we provide our draft BC-DR plan for the Kentucky Medicaid program and include a draft BC-DR specific to the Commonwealth.

PROPOSED EMERGENCY RESPONSE AND DISASTER RECOVERY PLAN

Our emergency response and DR activities are encompassed within our BC-DR plan, which includes processes for annual testing of business and system functions. The plan will ensure that critical processes and data are maintained for provider and Enrollee support services. It also defines protocols to notify providers and appropriate government agencies if an incident negatively impacts our business.

We will tailor our plan upon Contract award to meet specific Kentucky Medicaid program requirements. In accordance with program requirements, we will submit our BC-DR plan to the Commonwealth for review and approval during Readiness Review and annually over the course of the Contract. We will conduct tests at least once per calendar year and on an ad hoc basis through simulated disasters and lower level failures; business continuity exercises with the Incident Management team; and testing of critical system functions. Results will be made available to the Commonwealth upon request.

Molina IT Hybrid Cloud Solution

The strength of our BC-DR plan is based on the investments made to our IT infrastructure. We distribute technology systems and services enterprise wide across a hybrid cloud composed of four operating locations:

- **Primary:** Microsoft Azure South Central U.S.
- **Secondary/Disaster Recovery:** Microsoft Azure North Central U.S.
- **Systems:** Parent-company-owned-and-operated Data Center
- **DR:** Co-location Facility

Molina will continually optimize the distribution of services across the hybrid cloud to ensure the best Enrollee and provider experience. Exhibit E-1 shows the distribution of key services. All critical services are deployed into a primary and disaster recovery site and feature local high availability with remote disaster recovery. This means that Enrollees and providers will not typically experience outages outside of scheduled maintenance periods and declared disaster recovery incidents.

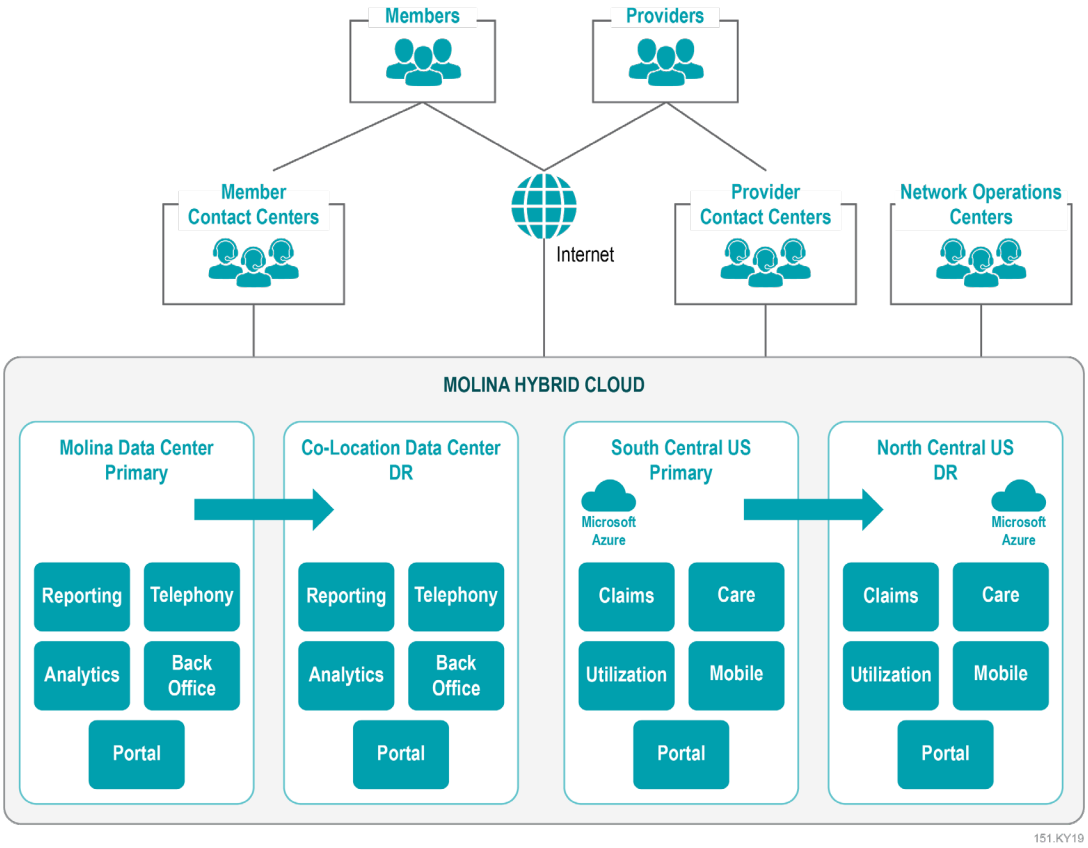


Exhibit E-1. Molina Hybrid Cloud

Disaster Recovery User Experience. The scope of any disaster will ultimately determine the impact; the general experience is described herein. Throughout some recovery activities, Enrollees and providers can expect communications systems such as telephones, fax services, and email to remain functional. We also have additional redundancy with satellite phones that were used in the hurricane disaster in Puerto Rico. These systems are supported by power generators (to provide phone service if electrical service is not available) and are designed to be fully redundant in multiple locations to route Enrollees, providers, and other users to the closest available system. Enrollee and provider Web portals as well as the transactional systems that manage claims, utilization, and care services will be unavailable until recovered. Once the DR plan has been invoked, restoration of these systems can be expected within 24 hours. Data will be current to just moments prior to the onset of the disaster. Reporting and analytics will be recovered after transactional systems, as highlighted in Table E-1.

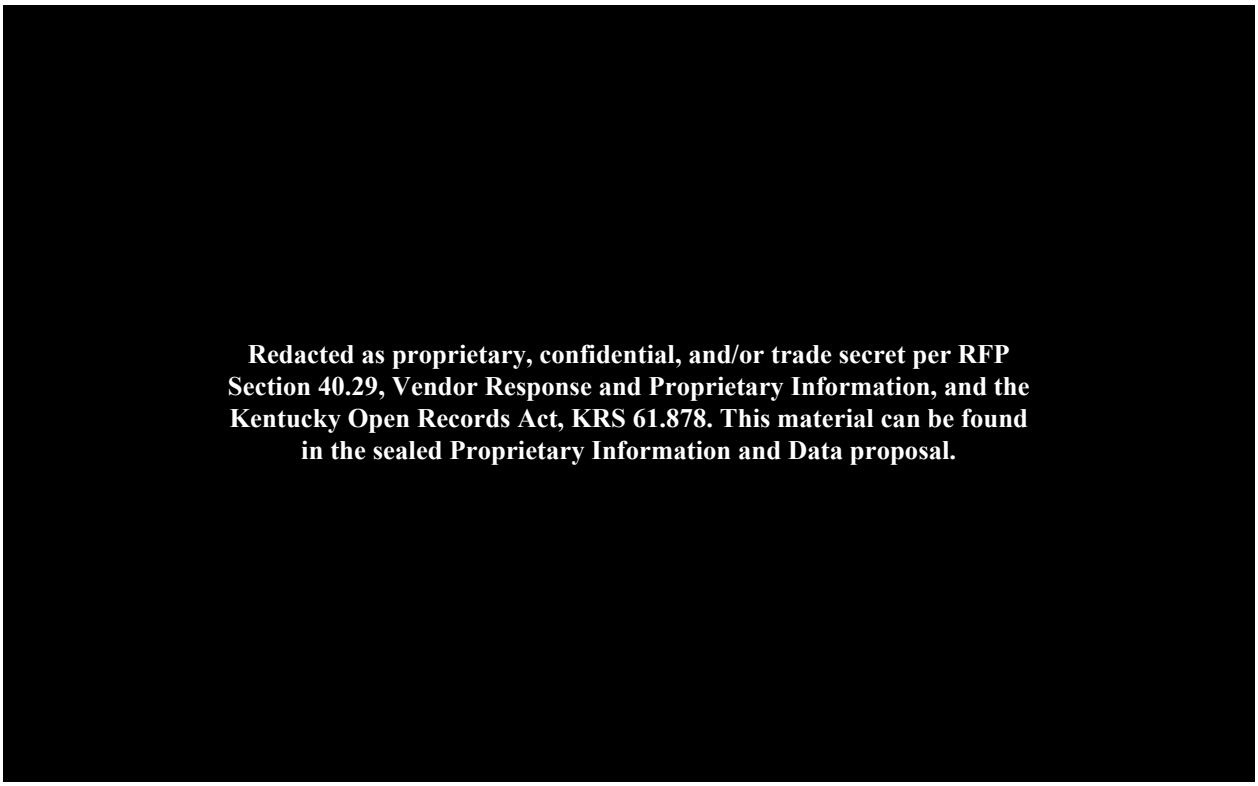
Table E-1. Expected Restoration of Services

System	Experience
Communications—telephone, fax, email	Available during recovery
Enrollee and provider Web portals	Restored within 24 hours
Transactional systems—claims, utilization, care	Restored within 24 hours
Reporting and analytics	Restored within 48 hours

We will configure our plan, in collaboration with the Department and including time frames of expected restoration of services, based on the Commonwealth's needs, while meeting and/or exceeding all Contract requirements.

System Highlight: Claims Management DR. This section highlights one system within the Molina environment; however, the architecture pattern is applied to many critical systems. Molina claims management services are comprised of web, file, application, and database servers. Each component of the architecture blends technology and process to ensure recovery. Procedural details are found in the DR plan. Exhibit E-2 illustrates the key technologies listed here:

- **Claims Management:** TriZetto QNXT
- **Web Server:** Microsoft Internet Information Services (IIS)
- **Operating System:** Microsoft Windows Server Datacenter
- **Database:** Microsoft SQL Server
- **Application Configuration Management/Deployment Pipeline:** Azure DevOps
- **Infrastructure Configuration Management:** Scalr and Salt
- **Recovery Technologies:**
  - Global Traffic Management: Azure Traffic Manager
  - File Replication: Azure Read-Access Geo Redundant Storage (RA-GRS)
  - Database Replication: Microsoft AlwaysOn Asynchronous Replication



User/Enrollee/Provider Recovery. Global Traffic Management redirects all users and service calls to the recovery site once all system functions are recovered and validated.

Web and Application Server Recovery. Configuration management tools ensure the primary and recovery sites always have the same code, configuration, and content. The web and application servers at the recovery site are always on; however, they do not process transactions until users, data, and services are re-routed during recovery activation.

File Recovery. Files stored on shared storage are replicated using Microsoft Azure RA-GRS (Read-Access Geo Redundant Storage). This ensures that files are replicated near real time. The file shares are always available and mounted to the recovery systems they support.

Database Recovery. SQL administrators promote the recovery database to primary. SQL AlwaysOn asynchronous replication ensures the recovery database is kept within a few transactions of the primary site. Network and processing latency can influence the actual differences between the two systems.

Risk Mitigation. A risk mitigation strategy is crucial as a part of the BC-DR plan. Risk mitigation helps to reduce and/or control the risk of threats. For example, the risk mitigation section addresses threats such as severe weather, power failure, IT application failure, flooding, and loss of access to the workplace. Specific risk mitigation actions included in our BC-DR plan include, but are not limited, to the following:

- The Network Operations Center to monitor voice communication equipment failure
- A defined Incident Management team for situations such as severe weather, and other natural threats
- Generator maintenance and uninterrupted power supplies to address a power failure and resulting damage
- Critical facility management to maintain controlled access to buildings and IT equipment rooms, as well as contracts with vendors for additional generators and fuel
- Redundant servers, server backups, database backups, data replication, DR infrastructure for critical applications, and application monitoring systems for IT application failure
- On-call subject matter experts and designated alternate Molina campuses or other facilities for relocation of staff (if necessary)
- Vendor support agreements (service-level agreements)
- Emergency Response teams for evacuation and shelter-in-place plans (fire, active shooter)
- Secure/locked containers in place (for storing sensitive records or data)

Telecom. The Molina telecom environment is comprised of integrated systems that control the voice communications for the professional- and Call Center-level applications. This environment is redundant at the infrastructure and application levels that span across two geographically separated data centers.

These features factor into the concept of disaster recovery for telecom, but the design is so much more than that. The Cisco voice systems co-exist in both data centers operating in an active-active environment. All components of the Unified Communications and Unified Contact Center solutions are designed to work in groups of subsystems that are ready at all times to handle operations if partner systems fail or otherwise become unavailable. From the Call Manager systems that control the desk phones to the user clients that allow agents to log into various call queues to handle calls, the systems are designed for redundancy controlled at the application layer.

What makes our telecom environment different from many other systems serving Molina is that redundancy is possible when the two halves of a complete solution operate as a whole with little human intervention to activate failovers.

Hybrid Cloud-Based Solution. Exhibit E-3 illustrates how moving to a hybrid cloud-based solution has further enhanced the redundancy and business resiliency of our operating environments. Microsoft Azure provides a cost-effective, scalable, versatile platform to maximize our technology service offerings. ***Recovery times and recovery point objectives (RPOs) are significantly reduced***. Our information and telecommunications systems, including Internet and telephone-based functions, are available to users 24/7 except during agreed-upon periods of scheduled system unavailability. We ensure that mission-critical systems that meet or exceed operational requirements are available. Cloud technology also provides enhanced security to protect data, including the tools for threat intelligence and analytics to quickly identify any threats and/or suspicious activity on the network.

Additionally, Data Center and Network Operations Center staff monitor systems, including applications, databases, network, and routers/switches. We also have a suite of proactive enterprise monitoring tools that monitor systems, applications, and infrastructure performance to provide early detection of episodes that impact operations.

We have also established a technology incident management process via an IT Service Management program, which allows for timely resolution of business-critical incidents.

We notify impacted stakeholders of incidents that affect business users and provide regular updates until issue resolution and provide a dashboard where real-time information, including network activity from our data center to our office locations, can be viewed.

Redacted as proprietary, confidential, and/or trade secret per RFP Section 40.29, Vendor Response and Proprietary Information, and the Kentucky Open Records Act, KRS 61.878. This material can be found in the sealed Proprietary Information and Data proposal.

1. ESSENTIAL OPERATIONAL FUNCTIONS AND RESPONSIBLE STAFF

Our Business Continuity Management team oversees and administers the BC-DR plan and offers extensive information technology, business continuity, and emergency management experience. We identify essential business functions and employees needed to address critical operations and support functions within our business continuity management plan. Our Business Continuity Management team maintains up-to-date information about our business processes. Business Continuity Management personnel also assemble and engage incident management teams at the corporate and local levels. During an emergency or other incident (e.g., inclement weather or a power outage), business recovery procedures enable operations to continue with minimal disruption.

In addition, care managers will prepare our Enrollees and their caregivers in advance by providing emergency contact information and by sharing expectations related to services and procedures. Partnering Enrollees and care managers also will provide Molina the opportunity to develop and document backup plans that address emergency disruptions. From transportation options to possible evacuation areas, each important detail will be documented in the Enrollee care plan.

In today's digital age, virtually every service has some supporting technology component. Molina's IT team supports all managed care program functions. The IT team continually strives to leverage the optimal technology to provide the best quality of service.

We highlight essential operational functions and responsible staff in Table E-2.

Table E-2. Essential Operational Functions and Responsible Staff

Essential Operational Function	Responsible Staff
Emergency Response	Emergency Management team (sub-unit of the Business Continuity Management team), facility managers, Emergency Response team
Business Continuity	Business Continuity team (sub-unit of the Business Continuity Management team), business leadership, Incident Management team, facility managers
Enrollee Disaster Planning	Molina Care Management staff
IT	IT Infrastructure teams, IT Application teams, DR team
Call Center	Enrollee and provider Call Center staff, Workforce Management team
Care Management	Molina Care Management staff
Claims Processing	Corporate Claims staff
Enrollee and Provider Grievances and Appeals	Enrollee and Provider Inquiry Research and Resolution staff
Pharmacy	Corporate Pharmacy and Pharmacy Operations staff
Provider Services	Provider Contracting and Provider Network staff
Quality Improvement (QI)	Corporate Quality and QI staff
Utilization Management	Molina Utilization Management staff
Web Portal	IT Corporate Application team

2. PLANS TO ENSURE CRITICAL FUNCTIONS AND CONTINUITY OF SERVICES

Our BC-DR policies and processes address accessibility and continuity of care management, utilization management, and pharmacy services for Enrollees and providers during business interruptions. This will ensure all critical business functions remain operational in the event of an unanticipated interruption to normal business operations, which may include a network outage, weather events, and medical, fire, and security emergencies. This plan will provide for the continuation of critical services when a business interruption occurs.

The Business Continuity team will collaborate with core teams such as the Enrollee Call Center, Healthcare Services, including Care Management and Utilization Management, and Medical Affairs to review impact to membership and develop the necessary work-around procedures to meet the needs of our most vulnerable Enrollees. We have identified recovery strategies to continue operating depending on the length of the incident. Departments have identified and documented operational business recovery procedures to restore each of the critical business functions. Disaster recovery plans are categorized by department, business function, and recovery time objective.

Ensuring Continuity of Care for Enrollees. Care managers and Utilization Management staff will be available during and after a disaster to help Enrollees and providers obtain necessary care and services. Care Management staff will work proactively with those vulnerable Enrollees in areas prone to significant weather events (e.g., flooding, tornadoes) to develop an action plan in the event of an emergency.

Additional information regarding emergency preparedness will be located on the Enrollee Web portal, the public website, and through the Molina Mobile app. Furthermore, during certain incidents, when the Enrollee calls into our Call Center, they will immediately hear a tailored message with pertinent incident information. Molina also has outbound SMS text message capabilities, and messages can be sent to Enrollees during an emergency. Helping Enrollees and the Commonwealth prepare by preplanning before a disaster is part of Molina's emergency response and disaster recovery plan.

The plan is given a prioritized leveling to ensure safety and that the resources to meet Enrollees care needs are accessible, including access to housing, food, medication, power sources for durable medical equipment, and identification of local emergency contacts and personnel to assist if needed. Utilization Management staff, the Clinical Pharmacy team, and medical directors will work with Government Contracts and Compliance teams to ensure regulatory approvals and prioritization take place during natural disaster events.

Care managers will inform Enrollees and caregivers of services and procedures during and immediately following an emergency, including targeted outreach to special needs Enrollees. To assist in emergency care planning, we will document in their file whether the Enrollee intends to evacuate or remain in their residence, and whether, during the emergency, their caregiver can take responsibility for services normally provided by our vendors or if we need to continue services. We will document the plan of care during and following an emergency.

Should operations cease due to a disaster, we will inform affected Enrollees and notify respective facilities where they receive services to help arrange for continued essential services. Our Care Management team's responsibilities following an emergency or disaster event will include:

- Contacting all Enrollees to ensure no changes in status or residence
- Identifying any immediate interventions needed and developing the Enrollee's plan
- Ensuring Enrollees displaced by disaster receive additional service coordination to meet current needs
- Ensuring Enrollees contacting our Call Center or Care Management staff receive expedited service coordination as determined by urgency of need

- Ensuring Enrollees relocated temporarily receive authorizations for service with non-contracted providers during a limited time frame while they establish a new residence and apply for new services; Enrollees will be provided with instructions on how to apply for services in their area of current residence

During an incident, we can also continue to provide support services to Enrollees through our Nurse Advice Line, our Behavioral Health Hotline, and through our national telehealth vendor to ensure continuity of care.

Continuity of Services to Providers. Providers will be contractually required to provide and coordinate all covered services to our Enrollees. Please note:

- Molina will not require prior authorization for medical services during disasters.
- Hospitals and providers will be expected to provide necessary services and advise us thereafter.
- Information regarding DR protocols will be available in the Provider Manual.
- We will alert the network of the incident and information regarding protocols via email / fax blast, the provider Web portal, provider Call Center, Molina Mobile app, and public website.
- Furthermore, during certain incidents, when a provider calls into the Call Center, the provider will immediately hear a tailored message with pertinent incident information.

Our Puerto Rico affiliate paid 409,211 claims totaling some $50 million from the time Hurricane Maria made landfall in September 2017 until year's end, which demonstrates our organization's ability to continually meet our contractual obligations even during times of great need.

Additionally, Molina has outbound SMS text message capabilities, and messages can be sent to providers during an emergency.

Molina also will provide education and training to providers to enhance awareness and help develop an understanding of emergency protocols and expectations. This training can occur through multiple modalities, including email / fax blasts, webinars, and in-person training conducted by staff at our six regional offices. We can also invite providers to participate in our proposed symposium to educate, train, coordinate, and plan as a cohesive front for any disaster that could affect Kentucky and its Medicaid population. This proposed format also will support cybersecurity and privacy.

Continuity of Pharmacy Services. When any of our service areas are affected by a disaster and a declaration of emergency is issued, our Pharmacy team will collaborate with the PBM to initiate standard operating protocols, which include allowing:

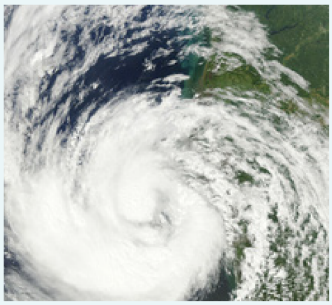
- Pharmacies to bypass early refill, prior authorization, and the non-formulary edit without having to call Molina or the PBM
- PBM pharmacy and Enrollee call centers to authorize medications that edit beyond the scenarios in the prior bullet on behalf of Molina
- Specialty and mail order programs to ship to alternative addresses to ensure continuity of care

The PBM will notify the pharmacy network of the above protocols via email / fax blast. It also will be posted on their website. The protocols also will be located within the pharmacy's provider manual.

Continuity of Services During a Disaster—A Puerto Rico Case Study

The case study in Exhibit E-4 demonstrates our organization's ability to effectively implement emergency/disaster protocols. While Kentucky may not be subject to the full force of a hurricane, the severe weather phenomena associated with it, such as high winds, tornadoes, flooding, utility outages, and the impact to citizens, are very real threats to the Commonwealth. Molina's Corporate Business Continuity Management team and local Molina resources will monitor weather-related conditions using a

tool that provides alerts from the National Weather Service. The tool specifies impacted counties and includes a map showing the path and severity of the hazardous weather, which will aid our preparation and communication efforts.



Hurricanes Irma and Maria caused widespread evacuations, flooding, power outages, and damage. Hurricane Irma was the first of two hurricanes expected to impact Molina in 2017. The BCM team activated the local IMT to begin preplanning utilizing the Incident Command System (ICS), which follows the FEMA National Incident Management System (NIMS). The preplanning included activating the BC plan, which addresses staff preparation at the office and home, notifying Commonwealth agencies, vendors, and placing critical Molina departments on standby to maintain business operations.

The office began preparations for damaging winds, heavy rainfall, and flooding. The local IMT and BCM team also contacted the Commonwealth and advised that preplanning was under way for continued services to enrollees and providers. **Molina was the first MCO to contact the Commonwealth with a proactive approach and to inquire about how Molina could assist the Commonwealth with disaster preparations.** Fortunately, Irma had minimal impact to Molina operations. However, with Hurricane Maria following close behind, and expected to be larger and more devastating than Irma, we continued with our preplanning. We collaborated with government agencies prior to each hurricane's arrival, as they moved through the area, and after the storm. When the Commonwealth activated its Emergency Operations Center, Molina was asked to have a representative onsite. Molina vendors were contacted to establish communication and to ensure they were preplanning and following their own BC plans to meet the needs of our enrollees and providers. Ensuring continuity of care was critical at that time, and our approach to DR and BC reflected its importance.

Prior to the hurricane's arrival, call center and claims processing were transferred to other Molina locations to maintain continuity of care. Hurricane Maria impacted five of the six locations; one location was severely impacted and unusable, while the others were damaged and temporarily offline. Business operations were transferred to other Molina locations per the business recovery procedures in-place to continue operations and service to our enrollees and providers. Molina staff were sent to the location not impacted by the hurricane to continue critical business functions while the remaining were sent to assist enrollees within the impacted area. Case managers ensured enrollee emergency plans were updated and encouraged the enrollees to follow them. Our mass communication tool assisted with employee accountably and manual procedures were used to reach out to those who did not respond. At completion of the hurricane incident, a debrief was conducted and an after-action report (AAR) was created to identify lessons learned.

Our initial post-hurricane efforts centered on a proposal to regulatory agencies whereby we assist agencies in disaster relief efforts for refugees in our assigned regions. We offered services to all refugees at the shelters we visited, regardless of whether they were our enrollees. We managed logistics, recruited our staff as volunteers, and provided preventive and emergency care (physical and mental) as well as coordination for social and clinical care. After an initial outreach to eight refugee shelters—where we attended to health-related concerns and distributed food, water, clothing, and other essentials—we extended our efforts to other municipalities outside of our regions in strong collaboration with our network. Our response included meeting with providers, increasing community engagement, providing transitions of care, conducting door-to-door check-ins with providers, and assisting providers with FEMA paperwork.

The strength of our plan is based on investments made to our IT infrastructure, which enabled us to stay operational during the likes of Irma and Maria, unlike our competitors. Our plan includes a strategy for restoring day-to-day operations, including alternative operational locations. Our plan also maintains off-site data backups that minimizes service disruptions or data loss due to system or program failures or destruction. We have built redundancy and business continuity into our operational environments within our primary and secondary data centers. As a result, we were able to continue processing claims amidst the hurricane aftermath resulting in continued operations and sustainability for our providers. **Molina was the first MCO to return to operations after the devastating Hurricane Maria.** If testing and preplanning activities were not exercised, the incident could have been much worse for our employees and enrollees.

339.KY19

Exhibit E-4. Continuity of Services During a Disaster—A Puerto Rico Case Study

3. STAFF TRAINING

Training will be provided to Molina staff responsible for BC-DR plan development and recovery procedures.

Topics will include:

- Individual responsibilities
- Commonwealth-specific processes
- Plan preparation, coordination, and communication procedures

Training can be accomplished online or onsite and will be supplemented by materials such as our BC plan.

Business Continuity Management personnel will have appropriate credentials and education/training to mentor and support the training needs of the Commonwealth and participants. Example credentials for personnel include:

- Certified Business Continuity Maturity Model Assessor from Disaster Recovery Institute
- Associate Business Continuity Planner from Disaster Recovery Institute
- ISO 22301 Lead Implementer from ICOR
- ITIL Foundation from ITIL
- First AID/CPR/AED Certification from American Red Cross (Emergency team resources)

Enrollee Services and Provider Services staff will be trained to respond to calls and can contact our organization's medical professionals as needed.

We will use a multifaceted training approach that follows Federal Emergency Management Agency (FEMA) recommendations. At the broadest level, we will conduct annual training to create awareness and promote preparedness. Pre-planning will enable us to remain focused on our Enrollees and their communities during emergency situations.

To bolster our overall employee preparedness, we will employ Emergency Response teams across the organization. These teams will include more than 450 employees trained in emergency procedures, first aid, CPR, and the use of automated external defibrillators, which will be installed in all Molina offices. Over the past three years, this training has been credited with saving the lives of one of our organization's employees and a neighboring tenant, demonstrating that our training has a beneficial impact on the wider community.

In addition, crucial employee leaders and employees in Enrollee- or provider-facing roles will receive specialized training at least annually. For example, Molina's care managers will receive emergency management training at the start of employment and annually thereafter.

Our Emergency Management and BC teams will develop and conduct training tailored to specific emergencies likely to occur in locations where we provide services. These teams will develop training for our Kentucky Medicaid program team, ensuring they have the tools, processes, and resources they need to provide the right response when it is most critical. Among the educational opportunities provided within our Regional Operations Center, Molina can provide emergency preparedness training for Enrollees, providers, and the Commonwealth.

Additionally, as described in greater detail in the testing description, our annual BC exercise will incorporate Incident Management team training, which will include topics such as Incident Management team roles and responsibilities, incident assessment, and incident action plan development, culminating in working through an exercise scenario. This training will ensure staff knows their role and exactly what to do in the case of an incident.

Should a natural disaster render the Commonwealth's Call Center inoperable, our Automatic Call Distribution will route callers to overflow call center operations throughout the United States to ensure seamless continuity of service for both Enrollees and providers. As such, we will cross-train teams across locations, so other parts of our organization will be ready to support the Kentucky Medicaid program at a moment's notice.

4. CONTINGENCY PLANS FOR COVERING ESSENTIAL OPERATIONAL FUNCTIONS

Our organization's comprehensive BC-DR plan and supporting policies detail the resumption of critical business functions and information systems in the event of a disaster. We have identified and trained Incident Management teams to execute necessary steps. Our recovery strategies consider loss of staff and loss of location scenarios. Many Molina employees will have the capability to work remotely, mitigating a situation where their workplace becomes unavailable. Employees in critical operational functions will be cross-trained at other locations, to allow the transfer of workload should one location be impacted by an incident.

Technology controls include high availability to maintain operations during minor disasters (e.g., a single floor or a single building is impacted by a virus attack or power outage), and a disaster recovery data center to support failover of critical systems.

Once life safety is ensured, greater focus will be placed on the resumption or continuity of business operations. The BC team will facilitate the various planning elements involved. Development and ongoing refinement of our program will be based on continually updated risk assessments and business impact analyses.

Risk assessments identify internal and external risks that can potentially impact business operations. By assigning a probability and impact to each risk, criticality can be established, which helps to rank the risks and prioritize mitigation efforts.

The business impact analysis identifies essential business functions and the potential impact an incident could have, which aids recovery prioritization. In addition, it captures IT applications and resources required to support business functions. The tool also maps out business and technological dependencies that allow for streamlined preplanning and incident mitigation.

As part of the business impact analysis, we analyze the impact of interruptions to key service requirements to set recovery time objectives and determine an optimal approach to risk mitigation and disaster preparedness. The risk assessment and business impact analysis will be updated at least annually.

The strategic objectives of the business impact analysis study identify the existence and relative criticality of the following key elements and determine the impact upon those elements of an unplanned disruption to normal business activities:

- Key business processes
- Key personnel
- Human resources policies
- Computer systems and recovery procedures
- Communication systems
- Interdependencies between key business processes, personnel, and computer and communications systems

- Vital records
- Dependencies upon critical vendors
- Worksite vulnerabilities
- Availability of alternate work facilities

Business recovery procedures are developed to prescribe steps to restore departmental operations.

Site risk assessments identify potential threats to business operations, their likelihood, impact, and mitigating controls. Business continuity plans pull all these components together, providing guidance and procedures to follow to address any incident, including steps for the Incident Management team to follow to assess the situation and develop an incident action plan.

Business continuity exercises facilitated by the BC team will validate the plans and provide training to Incident Management team members, fostering their readiness to address incidents using proven Incident Command System principles.

The BC team also will manage an enterprise mass notification tool that can send time-critical information to employees. All these Business Continuity Management program elements will ensure incidents cause minimal business interruption, so Molina can continue to provide services to Enrollees, providers, and the Department.

Detailed in Table E-3 is an overview of our contingency plans for covering essential operational functions in the event key staff are incapacitated or the primary workplace is unavailable.

Table E-3. Essential Operational Functions and High-level Contingency Plans

Essential Operational Function	High-level Overview of Continency Plan
IT	High availability; data replication; backups
Call Center	Cross-training of staff for active call sharing strategy across different sites
Care Management	Many staff work in the field and have remote capabilities; can work onsite if field work in impeded; office-based work can be handled by those able to work remotely
Claims Processing	Shared services geographically dispersed; cross-training among sites; redundancy built into electronic processing of claims
Enrollee and Provider Grievances and Appeals	Transfer workload to a non-impacted site
Pharmacy	Cross-training of staff; transfer workload across multiple locations
Provider Services	Staff have ability to work remotely or onsite; cross-training of staff
QI	Staff have ability to work remotely or onsite; cross-training of staff
Utilization Management	Cross-training of staff; transfer workload across multiple locations
Web Portal	Network redundancy; high availability; backups

5. APPROACH TO MAINTAINING DATA SECURITY DURING AN INCIDENT

To help provide continuous care and services, our BC-DR strategies include annual system testing to demonstrate system restoration as required.

IT services include, but are not limited to, core care and Web portal systems; infrastructure including servers, databases, telecommunications, network and data centers; daily help desk and desktop support; and support for regulatory submissions to state and federal entities.

Cybersecurity

Molina's Cyber Defense Center will monitor systems for unusual activity around the clock. Processes and procedures will be in place to prevent malicious acts and to remediate them when detected. The Information Security Incident Response plan will document the steps to take for remediation. For malicious acts by internal workforce employees, this will include engaging the individual's supervisor, and the Human Resources and HIPAA Program Management Office teams, in addition to the Cyber Defense Center's investigation. The individual will be closely monitored, and the user account will be disabled if necessary. Disciplinary measures, and possibly legal action, will be taken where appropriate. The workforce employee's workload will be distributed among the other members of his/her team to ensure continuity of operations.

More than an Ounce of Prevention

Simply preparing to recover systems and data isn't enough. We proactively monitor them, too. For example, Molina invested in a state-of-the-art enterprise command center that, among other functions, includes a computer incident response team to address cyber security threats as they materialize.

The Security Operations Center portion of our Cyber Defense Center will maintain constant vigilance for malware attacks. For suspected malware infections, the Computer Incident Response team of the Cyber Defense Center will investigate. For desktop or laptop computers, the infected device will be quarantined, a forensic analysis will be performed, and the computer will be reimaged. Infected servers also will be quarantined, including eviction from any cluster of which it may be a part. Cluster resources will be distributed across the remaining nodes. If the scale of the malware intrusion warrants it, systems may be failed over to the DR site. In all malware incidents, the Computer Incident Response team will conduct a thorough investigation.

Physical Security

Molina facilities will be protected with employee access card controls. The access system will be backed up to security servers and access panels to recover all access programming for the system. Should a power loss occur, all regular doors will revert to a "Fail Secure" mode allowing egress at all times and requiring a hard key for ingress. A security vendor will be called to the location to allow entry via a master key.

All fire doors will revert to a "Fail Safe" mode allowing egress and ingress through that specific door. In all emergency cases when the battery backup has been exhausted, a security vendor will be called to the location to monitor ingress and egress while the access system is unavailable.

Access control devices will be in place to secure information system hardware and protect data centers and equipment rooms. These devices may be electronic or mechanical. Only employees whose job duties require entry to these areas will be authorized and granted access.

Data Backup

Data backups will be performed on a server-by-server basis, so there will be some variations based on what is requested by the system owner. Typically, a full backup will be performed every weekend (termed "weekly"), and a differential backup will be performed nightly (termed "daily"). The first weekly backup of the month will be identified as the monthly backup.

Each backup will be retained at the primary data center for 35 days and duplicated to the DR site where it also will be retained for 35 days. Monthly backups will be archived at the recovery site and retained as required by the Molina Data Retention Policy. Per policy, files will not be stored on workstations, and backups will not be performed on workstations.

Business Continuity Management Software Tool

Our parent company has invested in an automated solution where all BC-DR plans are maintained, including planning components, such as the business impact analysis, key contacts and support for incident management, and annual exercises. This solution will be used for Molina and will provide an automated approach that will alleviate manual processes.

6. COMMUNICATION METHODS

Our BC-DR plan will indicate the order in which essential parties will be notified as well as time frames for notification. We will leverage appropriate communication channels to notify Enrollees, providers, and the Department. We also will alert the network of the incident and information regarding protocols via email / fax blast, the Enrollee and provider Web portals, all hotline numbers, and the Molina Mobile app.

Furthermore, during certain incidents when an Enrollee or provider calls into the Call Center, they will immediately hear a tailored message with pertinent incident information. Additionally, Molina will have outbound SMS text message capabilities where messages can be sent to Enrollees and providers during an emergency. Utilizing monitoring tools, our Network Operations Center will complete an initial assessment the moment a business interruption or disaster situation is discovered. Notification tools will allow the Business Continuity Management and Network Operations Center teams to then communicate essential information to key personnel identified within the plan and impacted stakeholders to begin mitigation.

Example Communication Methods

The following is an example of communication methods we will use as part of our short-term recovery strategy:

- Molina employees can work remote utilizing laptops (VPN) and cell phones. Working remotely, employees will have access to Molina file servers and state databases.
- Government Contract employees also will typically have laptops. Therefore, we will contact the Commonwealth via any available communication line to advise of status.
- Molina will build in additional redundancy with communication in the form of satellite phones, which were used during the hurricane disaster in Puerto Rico.

The coordinator of health plan communications will work to prepare ongoing status messages for providers through any available method of communication (e.g., website, fax blast) and act as a back-up to the hospital and provider contracting/services teams for phone calls, and so forth.

Business Interruption Notification Procedure

The Business Interruption Notification Procedure describes the process for requesting employee notifications via the Molina Incident Notification System (MINS) when an incident affects Molina or other enterprise location or causes a business interruption.

Business interruptions are incidents that have already caused, or have the potential to cause, a site to close, delay opening, or unable to conduct normal operations. These interruptions or incidents may include, but are not limited to, state of emergency declaration, weather, earthquakes, utility outages, security, IT interruptions, fire, or any other type of business interruption. An example of steps we will take for an Initial Incident includes:

1. Site management or designee at the location of the incident will send an email with the approved notification message to BCMTeam@MolinaHealthcare.com and will contact the Business Continuity Management team.
2. The Business Continuity Management team on-call person will be advised of the situation.
3. The Business Continuity Management team on-call person will then send the MINS notification to site employees.

4. Site management or designee will update the facility status line for employee updates.
5. The Business Continuity Management team on-call person will contact the Network Operations Center, requesting that an Alert Bulletin be sent with the approved notification message summary. The Alert Bulletin will go to all Molina employees.
6. The Business Continuity Management team on-call person will monitor the response rate to determine if the notification needs to be rebroadcast to those employees who have not confirmed receipt.

Emergency Notification System

Our emergency notification system will be used to broadcast critical information to employees and our Incident Management teams. The MINS will send emails, texts, and phone calls (personal and work) to our staff and will be tested biannually. We will use the Everbridge tool for emergency management.

Exhibit E-5. Everbridge Tool for Emergency Management

The tool will provide automated notifications to Commonwealth employees, and we will (assuming Enrollee consent) automate notifications and outreach that will ask for an Enrollee response (e.g., texting back “yes” or “no” to a question asking if they are okay and have what they need). This system will receive automated emergency notifications for all our locations in the Commonwealth relating to weather, law enforcement matters, and similar emergency scenarios. A mobile app will be available as part of this service as another method of notification if texting, email, and telephony are not appropriate or viable.

Exhibit E-6. Critical Event Management Platform

We also will maintain a facility status line that employees can call for information regarding the status of an incident that affects their business area, office, or location. In the case of a business interruption, specific operational departments will contact vendors to relay information regarding service interruptions. The incident notification tool also will have a conference bridge feature, allowing for support teams and business leadership to collaborate upon notification.

We will notify the Department regarding relevant and major incidents (e.g., critical operations like delivering services to Enrollees and stakeholders) by contacting relevant individuals per Contract guidelines. The BC-DR plan will include contact information for vendors, delegates, critical support teams and the Department.

7. TESTING PLAN

Our BC-DR plan will include annual testing of critical system and business functions. DR testing at various levels will be conducted each year to demonstrate our ability to restore system functions at the DR data center and ensure recovery time objectives and recovery point objectives are met. DR tests will involve system administrators remotely accessing production systems in the primary site and DR systems at the secondary site. Business users will be engaged at their respective office location, or may test from home, as the testing scope warrants. This will ensure our ability to provide access to critical information related to Enrollee and provider services. We will provide the results of this testing to the Department upon request.

An annual BC exercise will incorporate Incident Management team training, including topics such as Incident Management team roles and responsibilities, incident assessment, and incident action plan development, culminating in working through an exercise scenario. The exercise will address preplanning and assess our ability to transfer some or all operations to other locations, sustain operations over an extended period of time, and/or sustain operations with a reduced number of staff.

In Table E-4, we provide a sample summary of a recent BC-DR exercise accomplished at our Florida affiliate. As per the Molina Healthcare of Florida contract, the annual BC-DR test was completed prior to the April 30, 2019 requirement.

Table E-4. Molina Healthcare of Florida BC-DR Executive Summary

Overview	Outcomes
BC Exercise	
Objective	The annual BC exercise was successfully conducted on March 28, 2019. Objectives of the exercise included: • Activate the Incident Management team • Assign critical tasks using the Incident Command System • Analyze the situation • Evaluate business interruption response capabilities and state of readiness • Validate the BC plan • Provide input for continued strategic planning and training • Communicate with employees, partners, vendors, clients, and the community • Assess and maintain critical business functions • Manage personnel • Use manual work around procedures • Validate vendor contact information • Return to normal operations
Scope	Florida weather and manmade power incidents are common threats. Power incidents create a potential threat and direct impact to Molina Healthcare of Florida operations. The BC exercise demonstrates the use of communication tools, incident management, and activation of the BC plan.
Summary of the Exercise	The three-and-a-half-hour exercise scenario started with a power outage that began at 3:45 am, impacting the health plan. The exercise began with notification of the Incident Management team using the MINS. The power outage extended across two days simulating an impact to health plan operations. The Incident Management team used the BC plan to identify critical business functions. Departmental business procedures and the BC plan were used to preplan prior to the start of the business day. By use of the Incident Command System, incident responsibilities were assigned. Assignments included preplanning based on utility company estimated time to repair, vendor management, exercising downtime procedures, and using alternate Molina resources to meet the needs of health plan operations.
Exercise Results	The Incident Management team's assignment of tasks by utilizing the Incident Command System allowed for a structured and organized strategic response to an unplanned incident. The exercise demonstrated a plan to maintain business continuity of operations for Molina employees and members, and the organizational preparedness for successfully addressing a power outage.
DR Exercise	
Objective	The goal of the 2019 QNXT annual DR test was to demonstrate Molina Healthcare of Florida's ability to recover the QNXT version 5.3 production business applications from the Albuquerque, New Mexico, data center (DC01) to the DR environment in the Richardson, Texas, data center (DC02), and meet all objectives outlined below, thereby fulfilling Molina Healthcare of Florida's contractual obligation to annually conduct a DR exercise. • Objective One—24-hour Recovery Time Objective • Objective Two—24-hour Recovery Point Objective • Objective Three—Verify QNXT 5.3 Applications are Functional from DR Data Center
Scope	The scope of this testing was to ensure the QNXT application for the Florida health plan could be recovered from the Texas data center (DC02) to support business functions. The test included shutting down production servers, failing over the databases to Texas, and accessing the DR application servers. The business users from each state validated the DR environment, which included the lookup of a predetermined member, provider, claim, and call track for each state.

Overview	Outcomes
Exercise Results	The Molina Healthcare, Inc., QNXT annual DR test was executed on Saturday, April 20, 2019. QNXT is classified as a tier 1 application, with a recovery time objective and recovery point objective of 24 hours. The exercise was completed successfully, and the exercise objectives were achieved. Objective One—24-hour Recovery Time Objective • **Achieved**—The application was failed over and made available for business user validation much sooner than recovery time objective requirements. Objective Two—24 Hour Recovery Point Objective • **Achieved**—When the business users validated the data, they had production transactions from the time of failover available in DR. Objective Three—Verify QNXT Application is Functional in DR • **Achieved**—The business users completed validations to ensure the business applications were functional in the DR environment as expected.