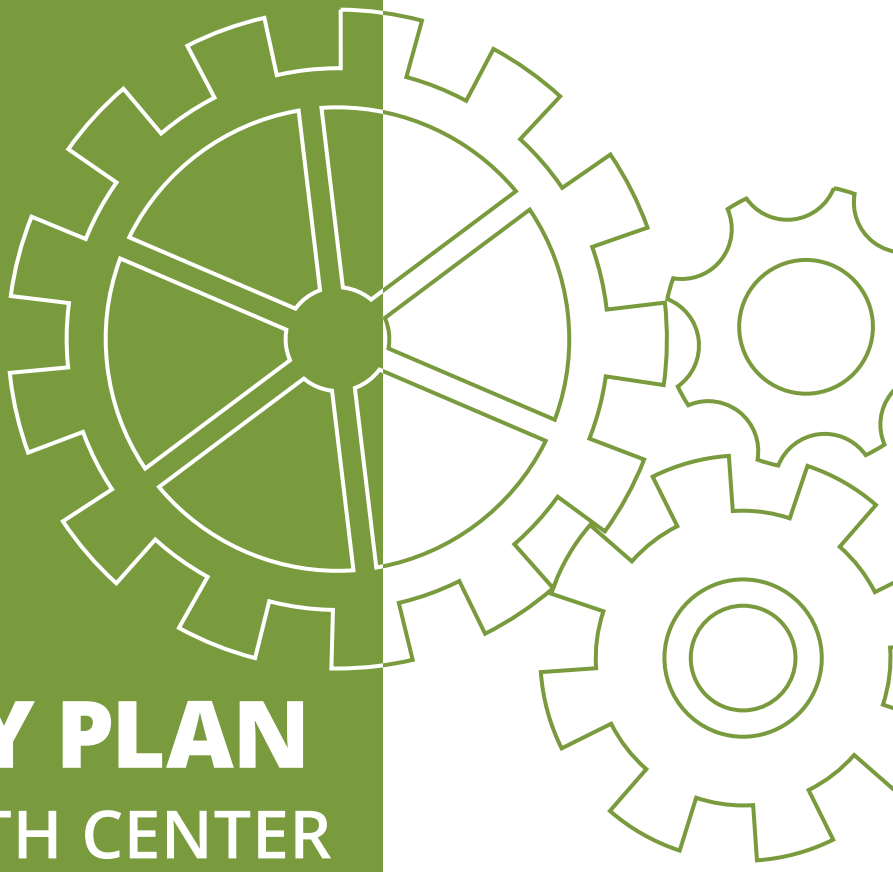
NATIONAL ASSOCIATION OF Community Health Centers



CREATING A BUSINESS CONTINUITY PLAN

FOR YOUR HEALTH CENTER

APRIL 2021

ABOUT THIS MANUAL

- This manual is the result of collaboration between the National Association of Community Health Centers (NACHC), Connecting Consulting Services, and Primary Care Development Corporation (PCDC).
- It is intended to provide community health centers and primary care associations an easy-to-use tool to create and/or improve their business continuity plan and program.
- For assistance, questions or more information on this and other business continuity and emergency preparedness tools and resources, please contact NACHC at trainings@nachc.org or 301-347-0400.

This publication is supported by the Centers for Disease Control and Prevention of the U.S. Department of Health and Human Services (HHS) as part of a financial assistance award totaling $2,000,000, with 100 percent funded by CDC/HHS. The contents are those of the author(s) and do not necessarily represent the official views of, nor an endorsement, by CDC/HHS, or the U.S. Government.

TABLE OF CONTENTS

BUSINESS CONTINUITY PLANNING

Business continuity planning is the process of identifying critical business functions of an organization, developing solutions to maintain those functions during a disruption, testing those solutions, and updating and revising solutions on a continuous cycle. The goal of business continuity planning is to enable critical business functions to continue uninterrupted during an emergency or disaster.

Threats to Business Continuity

Disasters can take many different forms, and the severity and duration of them can range from minor to catastrophic. Many types of disasters are unexpected (known as slow onset disasters) and leave communities in shock. To assist organizations in planning, disasters are divided into three main categories: natural, manmade, and technological.

Natural disasters are major adverse events that are caused by large-scale geological or meteorological changes in the earth. They can also be climatological or biological in nature. These can include:

- Avalanches
- Cyclones
- Disease Pandemics
- Droughts
- Earthquakes
- Extreme cold
- Extreme heat
- Floods
- Hail
- Hurricanes
- Insect/animal plagues
- Landslides or mudslides
- Sandstorms
- Severe storms (ice, thunder, etc.)
- Sinkholes
- Tornadoes
- Tropical storms
- Tsunamis
- Typhoons
- Volcanic eruptions
- Wildfires

Manmade disasters are those disasters that are caused by humans. Examples of manmade disasters are:

- Acts of terrorism
- Biological weapons
- Chemical spills
- Cyber attacks
- Groundwater contamination
- Mass shootings
- Radiological emergencies

A technological disaster is a non-natural event that can affect small and large areas, are frequently unpredictable, and can cause damage to property and loss of life. Examples include:

- Aviation, nautical, and railway accidents
- Dam failures
- Industrial pollution
- Nuclear radiation
- Toxic waste

Characteristics that Guide Continuity Planning

A solid business continuity plan (BCP) is needed to ensure health centers can restore operations quickly following a disaster. When developing our business continuity plans, the goal should be to create a plan that is comprehensive, realistic, efficient, and adaptable.

A comprehensive BCP is one that addresses as many different types of disruptions as possible. We cannot assume that an initial BCP will work for all scenarios. It is important to have back up plans should the initial plan fail.

It is also crucial that a BCP is realistic. When reviewing the types of disasters that may affect a health center, it's important to plan for those that are the most likely to occur. We must be realistic about the plan we have created and ensure that it has as many contingency plans built in as possible. During times of stress, even regular tasks can be more difficult to accomplish and, when a disaster or disruption occurs, we may not have long to act and implement our BCP.

It is vital to the success of a health center's planning to ensure that they can execute a BCP efficiently and with the resources they have on hand. Finally, health centers needs to ensure their BCP is adaptable. During a disaster or disruption, circumstances may change from minute to minute, so the plan should provide allowances for constant monitoring of the situation. As circumstances change, so should a plan.

THE IMPORTANCE OF BUSINESS CONTINUITY (BC)

At the time of the creation of this document in 2020, the year had already become forever etched in the collective memory as one punctuated by a global pandemic, 13 major hurricanes, and devastating wildfires throughout the country. Although where and when such events will strike, health centers should have the ability to continue to care for its patients through effective business continuity planning.

Unanticipated disaster events pose serious risks to our normal activities and operations. Common disasters can result in a crippling loss of facilities, critical processes and activities, communications, critical services (IT systems, data, power, vendor services), business equipment, business supplies, and in some extreme cases, people. Some organizations struck by disaster without adequate business continuity planning have suffered financial losses that have persisted for years. Other organizations simply never recover and ultimately close their doors. However, with proper planning and preparation, catastrophic outcomes such as these may be avoidable.

Business continuity plans are critical in keeping a health center open to provide care for the community when it is most needed following an emergency or other disruption. A BCP reduces the economic impact to the health center during a disaster and allows it to maintain its critical business and logistical functions. A solid BCP also helps health centers recover and get back to 'business as normal' more quickly and completely following an event.

A BCP and program is an ongoing process supported by senior management and funded by the organization. Critical processes that are necessary for the health center to continue services are identified, as well as how these processes will be maintained in adverse circumstances. Lastly, an effective business continuity process engages in a system of continuous training, testing, and maintenance of the plan and program.

A comprehensive and well-constructed BCP will:

- Augment good will, as well as, internal credibility with staff and external credibility with patients, vendors, and the community.
- Encompass a thoroughly researched, all hazards effort to ensure capabilities are developed to maintain business operations before, during, and after a disaster.
- Be communicated to the organization and obtain buy-in from essential stakeholders, such as leadership and/or senior management (this is most important), as well as, from the Board of Directors, staff, and vendors.
- Include consideration of all financial implications to continue the income flow, maintain a level of service to the community, and to keep staff whole.
- Bear community interests in mind, by maintaining a level of service to the community. Disasters are the time when communities need their local health systems the most.
- Recognize the positive effect a business continuity plan has after a disaster on reassuring and retaining qualified staff that are trained as well as maintain institutional knowledge and patient loyalty.

Goals and Objectives of a Business Continuity Plan

It is nearly impossible to predict with a high degree of certainty what type of disaster may strike, the timing, severity, impact, and duration of the disaster, and the resource requirements and availability for successfully recovering afterward.

> **A BCP is not intended to be an exhaustive "how to" manual, but rather to act as a realistic guide for good decision making, and to direct the actions of staff in the immediate aftermath of a disaster.**

The primary objectives of a Business Continuity Plan are to:

- Protect life and safety before, during, and after an emergency or disaster
- Safeguard and preserve our health center assets
- Minimize the impact of an emergency or disaster on our health center operations
- Minimize the time, effort, and uncertainty in reacting to an emergency or disaster situation
- Restore health center services and return to acceptable levels of operation in the short-term
- Return to normal business operations in the long-term

This BCP manual is intended to guide health centers in planning efficiently for disruption, thus minimizing downtime and maintaining operations during an emergency or other disruption.

BUSINESS CONTINUITY PLANNING
CASE STUDY

Utah Navajo Health Systems

During the COVID-19 pandemic, it was important to protect our staff, patients, and visitors to the highest extent as possible. In the initial weeks of the pandemic, our administrative team developed a plan to maintain business operations while still seeing patients inside our facilities. As our business continuity plan developed and unfolded, we made two main decisions regarding our business operations that aimed to protect everyone as much as possible:

1. **We utilized our parking lot as a triage location.** We developed a triage system to triage patients before they come into our parking lot. This allowed us to screen patients before they entered our facilities. Anyone exhibiting signs and symptoms of COVID-19 were isolated and brought into the facility through a separate entrance where they were placed in an isolation room. This worked out well and continues to work well. It is another measure to ensure patients are directed to the most appropriate part of our facility.
2. **We provided patients with their own pulse oximeter and thermometer to monitor themselves at home before calling 911 or going to the hospital/clinic.** This was a form of patient self-triage. This was extremely helpful in keeping our EMS services and clinics available for emergencies.

As we move into new phases of the pandemic, we adjust our business continuity plan accordingly. Some changes we plan to make in the future include purchasing and storing abundantly more PPE than before the pandemic, and continually evaluating our triage processes, both in our parking lot and other areas of our facilities.

CREATING THE BUSINESS CONTINUITY PLAN

The **business continuity plan (BCP)** is intended to be a dynamic plan and can be used in emergencies, disasters, and other catastrophic events where the technology, facility, or a department is severely impacted. BCPs are critical in keeping the facility open and providing care to the community. Having a BCP in place also reduces the economic impact to the health center during a disaster and allows it to maintain its critical business and logistical functions.

A business continuity plan should address these core elements:

1. Executive Summary
2. Form a Multidisciplinary Team
3. Conduct a Hazard Vulnerability Analysis (HVA)
4. Conduct a Cybersecurity Impact Analysis
5. Perform a Business Impact Analysis (BIA)
6. Develop a Mitigation Plan (strategies for identified risks)
7. Create Leadership Orders of Succession
8. Identify Recovery Strategies
9. Design Implementation Timeline (including education, training, and exercises)

1. Executive Summary

An Executive Summary is found at the beginning of a business continuity plan and includes the following key information:

- Description of a BCP
- What is contained in the plan and how it was created
- Why the BCP is important to the health center
- Who is covered under the plan and, in general, when, and how it will be executed
- Highlights the health center's commitment to continuity of business services during and after an incident
- Commitment to plan maintenance, training, and drills

Financial implications are usually a main motivator to keep your health center operational during a disruption. Statistics that can support buy-in for the BCP include:

- **25% of all small businesses never recover from a disaster.**
- **Health centers lose on average $12,000 to $30,000 each day they are closed.**
- **50% of businesses which sustain interruptions of a week or more due to problems at the primary site never recover.**

In addition, the following information may be used to justify the amount of time and funding required for a successful BCP:

- If the BCP is done well, the risk of disruption is considerably mitigated.
- The act of planning enables the health center to be better able to respond to a disruption, whether the type of disruption is specifically stated in the plan.
- The act of business continuity planning requires a good understanding of normal operations. This allows gaps, poor practices, and wasted resources to be identified so they can be addressed.

See Appendix B – Executive Summary Template

2. Form a Multidisciplinary Team

A robust BCP requires information on all aspects of the health center. Because of the detailed information needed from multiple departments, it is critical to approach the development and implementation of the business continuity plan with a multidisciplinary team. When building the Business Continuity Team (BC Team), it is important that they are able to work with and gather information from all the departments within the health center.

It is critical to ensure that the development of the BCP has administrative and executive support. A member of the health center's **senior management team** is responsible for overseeing the business continuity planning process. This leader's responsibilities may include:

- Establishing policy by determining how the organization will manage and control identified risks
- Allocating knowledgeable personnel and sufficient financial resources to properly implement the BCP
- Ensuring that the BCP is reviewed and approved at least annually
- Ensuring employees are trained and aware of their roles in the implementation of the BCP
- Reviewing the BCP testing program and test results on a regular basis

Under the direction of this BCP leader, the health center will identify a BC Team. This team maintains oversight of the BCP and should meet quarterly at a minimum. The planning team may include:

- Members from senior leadership (e.g. COO, CNE, CFO, CIO) or designees
- Emergency Preparedness Coordinator
- Appointed Business Continuity Manager
- Safety Officer
- Emergency Management Coordinator
- Facilities/Safety Manager
- Financial Services Manager
- Human Resources Manager
- IT Manager
- Risk Management
- Selected key service line and ancillary department managers

The BC Team will work with each department to identify the functions they need to be able to maintain operations and prioritize which functions are critical. Plans will be designed to ensure that these "critical functions" can be maintained during and after an incident.

Common scenarios causing a health center to be inoperable:

- Critical staff and/or vendors are unavailable or cannot be contacted
- Facility or the local community area is not accessible
- Equipment is not working at the health center
- Software is ruined or not working due to hardware issues or a cyber security attack
- Critical data and records are unavailable or destroyed
- Utilities are down

If a disaster occurs and the BCP is activated, emergency response procedures outlined in the emergency operations plan (EOP) will be initiated and the facility will activate the required Incident Command System (ICS). The leader of the BCP will coordinate continuity activities, including:

- Accessing essential recovery resources, including business records (e.g., patient medical records, personnel records, MOUs, purchasing contracts)
- Supporting the operations section
- Coordinating with the logistics section to restore business functions and review technology requirements
- Assisting other health center service lines and impacted areas with restoring and resuming normal operations

See Appendix C - Multidisciplinary Team Checklist

3. Conduct a Hazard Vulnerability Analysis (HVA)

The planning team members, in conjunction with other committees as needed (i.e. Environment of Care, Emergency Management, etc.), should conduct a hazard vulnerability analysis (HVA). This assessment is performed to identify and minimize risks/threats the health center may face and determine steps to minimize impact and maintain operations. The HVA process may include:

- Identifying risks (based on probability, history, and impact)
- Finding any control weaknesses and/or single points of failure
- Pinpointing, selecting, and documenting mitigation/corrective measure(s) (including costs) to mitigate the identified risks
- Reporting findings and identified risk(s) to the BCP leadership team and other health center stakeholders and personnel. Use an educational presentation to highlight the findings with a summary evaluation report, including mitigation strategies, that provides the leadership team with a formal written summary.

See Appendix E for an example of an HVA template and process for conducting an HVA.

4. Conduct a Cybersecurity Impact Analysis (CIA)

Healthcare organizations can experience significant breaches, with malicious criminals responsible for most incidents. Some areas of a healthcare organization are more appealing to cybercriminals because they collect financial and medical data, but all aspects of businesses that use networks can be targeted for customer data, corporate espionage, or customer attacks.

A cybersecurity impact analysis is a tool that is used to answer the following questions:

- Are there current and relevant threats?
- What internal and external vulnerabilities to a C-security attack exist?
- What C-security attacks could affect daily HC functions?
- What is the health center's risk comfort level?

See Appendix F- Cybersecurity Impact Analysis Template

5. Perform a Business Impact Analysis (BIA)

Once the HVA is complete, the team conducts a Business Impact Analysis (BIA). The BIA is a detailed study of all the business processes within the organization, department by department. Each department's processes are then analyzed to give the team a complete picture of a health center's critical (and non-critical) operations.

It is both necessary and helpful to create directions on how to perform the different processes, especially if they require specific steps. It is also important to understand any regulatory and legal requirements that apply to your specific health center, such as processes that must be maintained in a disaster or specific requirements to operate your health center at an alternate location.

The process may be divided into separate areas:

- **Critical Processes** such as patient registration or patient triage are essential functions that are important to the mission of the organization and must be maintained during an emergency event (Is it essential today to keep the business open?).
- **Non-Critical Processes** such as scheduling routine patient visits play an important function to the organization but are not essential during an emergency event to keep the business open.

When reviewing these critical processes for the BIA determine how limits of time and data may impact the maintenance of them:

- **Time** is analyzed to determine acceptable amount of downtime before this function is implemented.

  Recovery Time Objective is the maximum time and minimum service level allowed to restore a process following a disruption.

- **Data** analysis gives you what amount and type of data must be available so that you can still be open for business without severely impacting the business operations.

  Recovery Point Objective is the maximum period data may be lost from an IT service due to a disruption.

The team would then evaluate and document essential business functions including services, supplies, and vital records.

See Appendix G – Health Care Processes – Sample List

Business Impact Analysis Report

Upon completion of collecting data, documents and details for essential services, staffing, equipment and vital records, the Business Impact Analysis Report should be written to reflect all findings, gaps and areas that are well prepared and shared with the BCP leadership team and other key health center stakeholders. The report should include an executive summary that can be quickly referenced if an emergency occurs. The summary can include:

- Critical business processes and their priority level (e.g., low, medium, high)
- Names and contact information for the business continuity and the senior management teams
- Resources identified in the BIA process that are needed to continue doing business within the critical processes.
- Contact information for key contacts, vendors, and suppliers as well as back up.

See Appendix G -Business Impact Analysis Form

Mission – Essential Functions

- **Critical business functions** that must be done immediately or in less than four (4) hours. May present with immediate threat to life and health if interrupted.
- **Urgent business functions** that must be done between 4 – 24 hours or may present threat to life and health if interrupted.
- **Important business functions** that should be done between 24 – 96 hours or may present impact to operations and/or patient satisfaction.
- **Delayed business functions** have minimal impact and need to be done within 5-7 days.

Mission – Essential Equipment and Supplies

- Document status of **major equipment or critical supplies**, both on hand and in use, and how long they can operate with present supply of vital consumable materials. If it becomes necessary to relocate services to another facility, this list can be used as a starting point to ensure resources will be available.
- Take **inventory of current equipment and supplies** and create a **resupply list**.
- Check **condition of storage or onsite stockpiles** to determine the level of damage to equipment and goods after incident occurs.
- Document key external vendors needed to support essential functions and operations.

BUSINESS CONTINUITY PLANNING
CASE STUDY

Yukon Kuskokwim Health (Alaska)

Project Togo

Once we were given a date of when we would receive COVID-19 vaccines, we had to figure out a plan to get them to our patients in very rural parts of Alaska. Only 40% of the state is accessible by road and most villages are only accessible by plane or boat. Due to the time of year, we also faced the challenges of winter weather and mountainous terrain. We developed a plan to use small planes, amphibious vehicles, and snowmobiles and a small team to meet our patients where they lived. On our first airplane trip, the vaccine froze in the metal part of the needle when I was vaccinating on the tarmac and I had to keep it warm by tucking it between my coat and my shirt until right before we gave the vaccine. When we planned on meeting patients where they are, we meant it. We vaccinated people on snowmobiles, in their vehicles, on four wheelers, in airplanes standing in -20° F weather, in village clinics, and in their homes.

Due to our rural location, we were provided with a month's supply of vaccines at a time. It was imperative that none of the vaccines go to waste. It became a race against the virus. We named this project "Project Togo" after the hardiest husky in the 1925 sled mush to Nome. The husky ran 350 miles of the 1,150-mile trek from Seward, Alaska to Nome, Alaska on the Bearing Sea.

> "We had to figure out a plan to get them (COVID vaccines) to our patients in very rural parts of Alaska... We vaccinated people on snowmobiles, in their vehicles, on four wheelers, in airplanes standing in -20° F weather, in village clinics, and in their homes."

Mission – Essential Vital Records

Identify, protect, and make readily available electronic and hardcopy documents, records, information systems, and data management software needed to support essential functions during emergency response and recovery. Data and documents include:

- Policy and procedures
- Emergency Operations Plan
- Admission records
- Licenses (i.e., RN, LVN, MD, etc.)
- Timecards
- Patient records

Mission – Essential Staffing

Work with senior leadership and key departmental mangers/directors to identify essential staff that are needed within the health center and specific departments to maintain operations. Evaluating this before a hazard or crisis strikes may assist with continuity of operations by:

- Evaluating current staffing levels and resource deployment needs post incident
- Notifying key stakeholders and personnel as to status and plan implementation.
- Notifying employees regarding plan activation and process.
- Implementing alternative staff resource options.
- Evaluating immediate and ongoing staff needs.
- Identifying contractors or other staff options that may mitigate problems resulting from staff loss.
- Identifying work options available through "telecommuting" or other off-site possibilities.
- Assessing flexible leave options.
- Assessing union issues regarding personnel issues.
- Evaluating potential health and safety issues that may arise.

6. Develop Mitigation Strategies

Once you have completed the Business Impact Analysis for all the departments within your health center as well as the BIA report and BIA summary, you will see where you should protect your business assets to prevent or minimize downtime during a disruption.

The BC Team should look at creating mitigation strategies, procedures, protection, and backups for the health center, such as:

- Reinforcing internal and external structure at the physical site
- Ensuring fire detection and suppression systems are current and operable
- Developing redundant third-party support
- Developing back-up systems and procedures for computers and software

Create mitigation strategies and procedures that support business processes of the health center:

- Procedures to incorporate appropriate inventory of critical equipment
- Maintain adequate supplies of water, non-perishable food items, batteries, and medical supplies
- Develop offsite backup systems for data, critical software, and facilities
- Develop disruption alternatives for:
  - Power
  - Communications
  - Data and records, and recovery of information
  - Facility
  - Staffing

It is also helpful to design a mitigation policy for the health center to identify and guide the strategy for accomplishing these activities. This policy should outline the importance of mitigation (and the health center's commitment to furthering it), and include a list of mitigation measures, the party responsible for overseeing its completion, and a timeframe for completion.

See Appendices H - Emergency Communications, Policy, and Procedures, I - Risk Communications, and J - Mitigation Plan to assist with mitigation planning efforts.

7. Create Leadership Orders of Succession/Delegations of Authority

Continuity of leadership during an emergency is critical to ensure continuity of essential functions. It is important to establish and maintain **Orders of Succession** ahead of time for key positions in the event leadership is incapable of performing authorized duties. The designation as a successor enables that individual to serve in the same position as the principal in the event of that principal's death, incapacity, or resignation. Roles should be identified by position title and not by name. There should be at least three different persons identified as successors for the role:

EXAMPLE

KEY POSITION	SUCCESSOR 1	SUCCESSOR 2	SUCCESSOR 3
EXAMPLE Chief Executive Officer	Chief Operating Officer	Chief Financial Officer	Chief Nurse Executive

Delegation of authority allows certain duties of one individual/position to be divvied up and assigned/delegated to multiple individuals. This occurs if the designated successor is not available or based on expertise of other facility personnel. Delegations of authority provide successors the legal authority to act for specific purposes and to carry out specific job duties. Example below:

EXAMPLE

AUTHORITY	TRIGGERING CONDITIONS	POSITION HOLDING AUTHORITY	DELEGATED AUTHORITY
Close and evacuate the facility	When conditions make coming to, or remaining in, the facility unsafe	Chief Executive Officer	1. Chief Operating Officer 2. Safety Officer 3. Engineering Director
Represent facility when engaging government officials	When the pre-identified senior leadership is not available	Chief Executive Officer	1. Chief Operating Officer 2. Public Information Officer 3. Risk Management Director
Activate facility MOUs	When the pre-identified senior leadership is not available	Chief Executive Officer	1. Chief Operating Officer 2. Finance Director

8. Recovery Strategies

Based on the identified risks outline in the BIA summary report, the BC Team will also recommend **recovery strategies to help the health center return to partial and/or normal operations following a disruption**. Business disruptions generally fall into one or more of the following categories:

- Facility
- Equipment
- Staff
- Technology

Recovery strategies may include:

- Determine and test manual/downtime workarounds, maximum tolerable downtime (MTD), recovery time objectives (RTO) and recovery time actual (RTA), and recovery point objectives (RPO)
- Establish patient recovery and strategies to bring them back into the health center
- Identify and document reimbursement and cost recovery strategies (e.g. FEMA reimbursement)

Special Note: These can be incorporated into a separate policy or included into the Emergency Operations Plan (EOP).

Recovery strategies and procedures can be developed for different disruptions and should cover almost every situation that your business may encounter. A **disruption action plan** should be developed for each situation and ensure that there is a current inventory of the critical assets required to enable business processes to continue.

For each piece of equipment make sure to record information required to make service calls quickly in the event of a disruption such as:

- Equipment: List the type of equipment and location
- Serial Number/Key/License: Identification numbers for the equipment
- Company: Vendor/manufacturer
- Warranty: Warranty expiration date. If no warranty, enter "n/a"
- Service contract/Vendor: Company name and contact information
- Notes: Any additional information

9. Plan Sustainability

Part of business continuity planning must be a commitment to sustain the work the team has done. This should be incorporated into a policy that includes:

- Identification of the BC Team who will be responsible for sustaining the BCP after it is completed
- A senior leader "champion" who can assist when necessary to maintain BCP efforts (i.e., Business Continuity Plan Coordinator, Emergency Management Coordinator, etc.)
- Who is responsible and how frequently the plan should be reviewed
  - What events (drill, actual disruption, etc.) would trigger a review of all or part of the plan outside of the normal review schedule
- How staff will be trained on the plan including frequency of training, who is responsible for overseeing the training, and which staff will be trained on specific topics
- How staff will be drilled on the plan (i.e., in-person and in groups/teams, self-directed/self-paced with an online learning series), frequency of drills (at least annually or as needed after incident occurs).

It is critical that during the development of the BCP, the BC Team set dates, times, and topics for BCP trainings, drills, and team meetings to review the plan. This will ensure that it can be incorporated into the normal schedule of operations at the health center. By making this part of routine health center operations approved by senior leadership, will help to ensure the senior leadership's commitment to sustaining the work of the team.

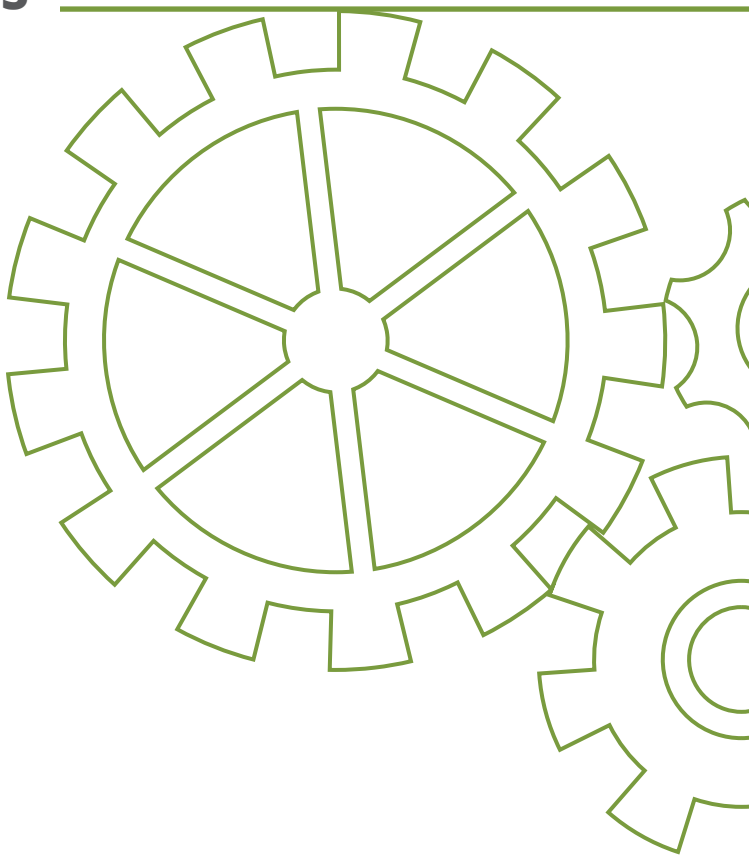
Teams should also track all changes to the BCP. Health centers can choose a method that works for them, however two suggested methods include:

1. Maintaining a revision page within the BCP that lists changes and updates. It should include a description of the change, date of change, and the person making the change.
2. At the bottom of each policy, insert a space titled "Last Updated" and record the date of the last revision.

Create a Transition Schedule so that the BCP Plan is reviewed and revised periodically by assigned Staff and /or the BC team.

See Appendix O – Transition Schedule

APPENDICES



APPENDIX A ⟩ KEY TERMS

Business Continuity	The capability to continue essential business processes under all circumstances.
Business Continuity Plan	Well researched, all-hazards effort to ensure capabilities are developed to maintain business operations before, during and after a disaster. Consists of a business impact analysis (BIA), hazard vulnerability assessment (HVA), and impact scenarios.
Business Impact Analysis (BIA)	The process of identifying and quantifying the impacts of an emergency or disaster in both financial and non-financial terms on an organization. It considers essential critical processes that are required to conduct business during an emergency event.
Critical Process	Essential functions that are important to the mission of the organization and must be maintained during an emergency event.
Emergency	A condition of disaster or of extreme peril to the safety of persons and property caused by natural, technological, or man-made events that may have a quick or slow onset.
Emergency Management Plan (EMP)	The plan developed for organizations that identifies how the organization will respond to all disruptions or emergencies. Also called an Emergency Operations Plan (EOP).
Executive Summary	Demonstrates that the Business Cowwntinuity Plan is an ongoing process supported by senior management and is funded by the organization. It is usually the introduction to the plan.
Hazard	A potential or actual force with the ability to cause loss or harm to humans or property.
Hazard Vulnerability Analysis (HVA)	An event-focused, systematic approach to identify, assesses, and prioritize each hazard that may affect a health center. It identifies the health center's vulnerabilities. The vulnerability is related to both the impact on the organizational function and the likely demands created by the hazard impact.
Process	A systematic series of activities or tasks that produce a specific end.
Risk	The effect of hazard combined with vulnerability.
Vulnerability	How susceptible resources are to the negative effects of hazards including the likelihood of a hazard occurring, and the mitigation measures taken to lessen the effects of hazards.

APPENDIX B ⟩ EXECUTIVE SUMMARY TEMPLATE

Insert Health Center Name

The Business Continuity Plan (BCP) for insert healthcare center name has been developed to address what is necessary to resume business operations as quickly and efficiently as possible after an emergency event. The insert healthcare center name has determined the need for a comprehensive BCP which includes:

- Top Reason #1
- Top Reason #2
- Top Reason #3
- Top Reason #4 (optional)
- Top Reason #5 (optional)

Both a business impact analysis and all-hazards planning approach have been used as the foundation of the plan. This BCP supports insert healthcare center name efforts to prepare and maintain all essential business functions and supporting dependencies (i.e. equipment, supplies, records) necessary to support healthcare operations in the event of an emergency. This BCP enables each staff member and department to be prepared for all emergencies that may occur, including natural, technological, or human induced disasters.

The insert administration name requires the active cooperation and commitment from all departments and employees in the preparation and maintenance of the plan. The BCP is to be incorporated into job duties at all levels, and staff will be trained and exercised accordingly in order to support the plan. Further, staff response will become incorporated into overall job performance evaluation, and an ongoing dialogue and feedback on the matter will be encouraged. This will ensure a successful implementation of the plan.

Health center senior leadership and the Board of Directors support the Business Continuity Plan in the promotion of diligent mitigation and efficient response as well as the maintenance and resumption of business operations to the community as soon as possible after an emergency.

CEO / Executive Director / etc. Date

Chair, Board of Directors Date

APPENDIX C ⟩ MULTIDISCIPLINARY TEAM CHECKLIST

Insert Health Center Name

	MEMBER ROLE	NAME	TITLE	EMAIL	PHONE
❑	Senior leadership (e.g. COO, CNE, CFO, CIO)				
❑	Emergency Preparedness				
❑	Business Continuity Manager				
❑	Safety Officer				
❑	Emergency Management Coordinator				
❑	Facilities/Safety Manager				
❑	Financial Services Manager				
❑	Human Resources Manager				
❑	IT Manager				
❑	Risk Management				
❑	Other Key Services Line Managers				
❑	Other Key Services Line Managers				
❑	Other Key Services Line Managers				
❑	Other Key Services Line Managers				

APPENDIX D ⟩ HEALTH CARE PROCESSES SAMPLE LIST

HEALTH CARE PROCESSES			
❑	**Legal and Regulatory Requirements**	❑	**Human Resources** • Payroll • Staffing
❑	**Clinical** • Patient care • Customer/Patient service • Clinical orders • Protocols • Treatment plans • Clinical decision support • Medical and clinical documentation	❑	**Administration** • Scheduling • Registration • Documentation of patient encounters • Patient records management • Procurement • Inventory • Supply chain processes
❑	**Financial Accounting** • Insurance claims processing • Account receivable • Accounts payable • Health center insurance	❑	**Facility Maintenance** • HVAC • Utilities • Housekeeping
❑	**Information Technology** • Hardware • Software • Back ups • Communications: online, wireless, POTS, PBX	❑	**Data Warehousing** • Medical treatment results • Lab data • Billing data • Patient file

APPENDIX E ⟩ HAZARD VULNERABILITY ANALYSIS TEMPLATE

Insert Health Center Name

Identification of Natural, Technological, and Human Made Hazards

POTENTIAL DISASTER	PROBABILITY RATING	AVERAGE IMPACT RATING	AVERAGE MITIGATION RATING	BRIEF DESCRIPTION OF POTENTIAL CONSEQUENCES & MITIGATION ACTIONS
Natural Hazards Probability: 1= Very Low to 3= High | **Impact:** 1= Minor annoyance to 3= Total destruction				
Example: Wildfire	3	3		Building inaccessible; personnel and IT potentially affected
Technological Hazards Probability: 1= Very Low to 3= High | **Impact:** 1= Minor annoyance to 3= Total destruction				
Human Made Hazards Probability: 1= Very Low to 3= High | **Impact:** 1= Minor annoyance to 3= Total destruction				

Hazard Vulnerability Assessment Summary Results

The sample HVA revealed that the **highest risks** were:

- **Natural Hazards –** Earthquake (78%), Gas Main Break (56%), Thunderstorm (37%), Internal Flood (22%) and Fire (20%).
- **Technological Hazards** Failure (56%), Electrical Failure (52%), Elevator failure (48%), Communications Failure > 4 hours (41%), and Information Technology Failure (33%)
- **Human Caused Hazards-** Pandemic (72%), Violent Person (50%), Train crash (22%), CBRNE Exposure (24%), and (19%), and Bomb Threat (17%).

APPENDIX F ⟩ CYBERSECURITY IMPACT ANALYSIS TEMPLATE

Insert Health Center Name

A cybersecurity incident is likely to cause harm to critical functions and services by impairing or compromising the confidentiality, integrity, or availability of electronic information, information systems, services, or networks, or diminishing the security facility. Healthcare facilities experience significant breaches, with malicious criminals responsible for most incidents. Some of these sectors are more appealing to cybercriminals because they collect financial and medical data, but all businesses that use networks can be targeted for customer data, corporate espionage, or customer attacks. Compromise can occur through various means, such as unauthorized access to information, hacking, phishing, and loss or theft of laptops, among others. The following checklist provides introductory methods that can be implemented to protect the facility in this digital frontier.

ACTIONS TO PROTECT COMPUTER HARDWARE AND OTHER TECHNOLOGICAL EQUIPMENT FROM CYBER THREATS

- ❑ Identify lost or stolen laptops and devices immediately; establish appropriate procedures to report lost items for employees
- ❑ Develop and implement procedures to prevent unauthorized data transfer via USB drives and other portable drives as well as cloud storage
- ❑ Wipe content on all devices before they are discarded or transferred to others
- ❑ Establish policies and procedures to disable inactive accounts, including those of transferred or terminated employees, after a set time period
- ❑ Set automatic timeouts for all computers following a period of inactivity
- ❑ Monitor, log, and report all intrusions to the appropriate authorities
- ❑ Review manufacturer technical safeguards, standards, and incident reports of all medical devices that are issued to patients to reduce malware and other security risks
- ❑ Develop and implement a detailed plan of how to address potential cybersecurity vulnerabilities with medical devices

ACTIONS TO PROTECT LOCAL NETWORKS AND OTHER COMPUTER SOFTWARE FROM CYBER THREATS

- ❑ Conduct a computer network assessment to obtain the information you need to develop a cybersecurity plan to reduce cyber threats, cyber attacks and address breaches
- ❑ Encrypt all computers and mobile devices issued by the organization and establish methods to preapprove the use of any devices not issued by the organization
- ❑ Implement role-based access to any systems to ensure employees only have access to any programs and applications necessary to perform the functions of their job
- ❑ Establish methods to prevent the installation of any unauthorized software applications
- ❑ Perform regular desktop audits for the entire organization to ensure unauthorized software applications are not installed
- ❑ Install and regularly update anti-virus software on all network computers

- ❑ Conduct anti-virus scans on all incoming and outgoing files
- ❑ Perform regular email "phishing" drills to educate and promote awareness of the risk of threats coming in through email
- ❑ Continue to research and build the necessary firewalls to protect against intruders
- ❑ Develop security policies for the use of virtual private network or remote connections
- ❑ Configure any electronic health records (EHR) system or database to require specific access permissions for each user; inquire with the EHR vendor to determine how they provide updates and technical support
- ❑ Backup data regularly and develop a plan to access information quickly in case of a natural or manmade disaster

ACTIONS TO ENCOURAGE SAFE CYBER PRACTICES FROM EMPLOYEES

- ❑ Define policies and procedures for employee use of your organization's information technologies
- ❑ Employ a system notification banner before granting employees access to the system that informs them of applicable regulations and federal laws (i.e. system usage may be monitored, recorded, and subject to audit and unauthorized use of the system is prohibited and subject to criminal and civil penalties)
- ❑ Conduct information and cyber security awareness trainings and workshops to educate employees about phishing scams, spyware, and identity theft on initial hire and on annual basis; employees should also be aware of how to report and respond to suspicious cyber events
- ❑ Require employees and staff to utilize strong passwords for networks and systems with a combination of letters, numbers, and special characters
- ❑ Require frequent password changes for all systems
- ❑ Implement multiple authentication methods for computers and networks
- ❑ Establish policies prohibiting the transmittal of protected health information using unencrypted public networks (i.e. free Wi-Fi hotspots)

KEY CYBER SECURITY INCIDENT DEFINITIONS

Cyber Crime: A criminal act involving computers or computer networks. Cyber crimes can be comprised of cyber attacks such as stalking and distribution of viruses and other malicious code or traditional crimes (e.g. bank fraud, identity theft, and credit card account theft).

Cyber Attack: An act, usually through the Internet, that attempts to undermine confidentiality, integrity, or availability of computers or computer networks, or the information that resides within the systems themselves. A cyber attack is sometimes referred to as hacking.

Malware: An umbrella term that describes all forms of malicious software designed to wreak havoc on a computer. Common forms include viruses, trojans, worms and ransomware.

Virus: A type of malware aimed to corrupt, eraseerase, or modify information on a computer before spreading to others. However, in more recent years, viruses like Stuxnet have caused physical damage.

Ransomware: A form of malware that deliberately prevents you from accessing files on your computer – holding your data hostage. It will typically encrypt files and request that a ransom be paid to have them decrypted or recovered.

Trojan Horse: A piece of malware that often allows a hacker to gain remote access to a computer through a “back door”.

Worm: A piece of malware that can replicate itself in order to spread the infection to other connected computers.

Bot/Botnet: A type of software application or script that performs tasks on command, allowing an attacker to take complete control remotely of an affected computer.

Spyware: A type of malware that functions by spying on user activity without their knowledge.

Phishing or Spear Phishing: A technique used by hackers to obtain sensitive information. Such as using email messages designed to trick people into divulging personal or confidential data such as passwords and bank account information.

APPENDIX G ⟩ BUSINESS IMPACT ANALYSIS TEMPLATE

Health Care Processes – Sample List

1. Using the Sample List to get you started, check off all the departments you have in your organization that is on the list.
2. Write in any departments that your organization may have that are not on the Sample List.

Insert Health Center Name

HEALTH CARE PROCESSES DEPARTMENT LIST			
❑	**Legal and Regulatory Requirements**	❑	**Human Resources** • Payroll • Staffing
❑	**Clinical** • Patient care • Customer/Patient service • Clinical orders • Protocols • Treatment plans • Clinical decision support • Medical and clinical documentation	❑	**Administration** • Scheduling • Registration • Documentation of patient encounters • Patient records management • Procurement • Inventory • Supply chain processes
❑	**Financial Accounting** • Insurance claims processing • Account receivable • Accounts payable • Health center insurance	❑	**Facility Maintenance** • HVAC • Utilities • Housekeeping
❑	**Information Technology** • Hardware • Software • Back ups • Communications: online , wireless, POTS, PBX	❑	**Data Warehousing** • Medical treatment results • Lab data • Billing data • Patient file

Insert Health Center Name

BUSINESS IMPACT ANALYSIS FORM

DEPARTMENT: _____

BUSINESS PROCESS: _____

TYPE: CRITICAL PROCESS NON CRITICAL PROCESS

PRIORITY: HIGH MEDIUM LOW

DESCRIPTION: _____

NUMBER OF PATIENTS AND/OR STAFF AFFECTED: _____

EMPLOYEE(S) IN CHARGE: _____

PROCESS INFORMATION

RECOVERY POINT OBJECTIVE: TIME: ___ HOURS ___ DAY(S) ___ WEEK(S) ___ MONTH(S)

RECOVERY TIME OBJECTIVE: TIME: ___ HOURS ___ DAY(S) ___ WEEK(S) ___ MONTH(S)

SERVICE LEVEL: _____

IS THIS FUNCTION A GRANT DELIVERABLE? NO YES – **Which grant(s)?**

IS THIS FUNCTION REQUIRED BY LAW/REGULATION? NO YES – **Which governmental agency?**

RESOURCES REQUIRED FOR RESUMPTION AND RECOVERY

- ❑ Personnel: _____
- ❑ Vendor(s)/outside provider(s): _____
- ❑ Key contact(s): _____
- ❑ IT hardware and software: _____
- ❑ Records (electronic or paper): _____
- ❑ Medical equipment: _____
- ❑ Medical supplies: _____
- ❑ Facility/office space: _____

PLAN FOR SHORT TERM (< 3 DAYS) DISRUPTION:

_____

PLAN FOR LONG TERM (> 3 DAYS) DISRUPTION:

_____

APPENDIX H ⟩ EMERGENCY COMMUNICATIONS POLICY AND PROCEDURES

SCOPE

To provide safety and response for __insert healthcare center name__ personnel during an emergency or disaster as part of _insert healthcare center name_'s disaster plan.

PURPOSE

This Emergency Communications Policy and Procedures includes instructions for health center leadership to communicate with staff, patients, contractors and other entities, external partners, and any volunteers during an emergency.

DEFINITIONS

Activation notification: A notification category that provides urgent information about an unusual occurrence or threat of occurrence, and orders or recommends that the notified entity activate its emergency response (usually via its emergency operations plan). An activation notification may indicate a **partial** or **full** activation It usually includes actionable information directing the notified entity on initial actions for mobilization, deployment, and/or response.

Advisory: A notification category that provides urgent information about an unusual occurrence or threat of an occurrence, but no activation of or response by the notified entity is ordered or expected at that time.

Alert: A notification category between "advisory" and "activation" that provides urgent information and indicates that action may be necessary. An alert can be used for initial notification that incident activation is likely, and for ongoing notification throughout an incident to convey incident information and directed or recommended actions.

Common terminology: Normally used words and phrases—avoiding the use of different words/phrases for same concepts—to ensure consistency and to allow diverse incident management and support organizations to work together across a wide variety of incident management functions and hazard scenarios.

Communications: A structured mechanism for transmitting information. "Communications" is a narrow but vital element of information management, referring only to the method(s) for conveying information. The process of transmission of information through verbal, written, or symbolic means.

Public information – The responsibility to accurately and promptly inform relevant stakeholders about an incident such as a hurricane, earthquake, bomb threat, fire, or terrorist incident that threatens health, safety, property, the environment, and/or critical operations.

Crisis communication – The communication strategy and accompanying tactics deployed to help an organization facing a challenge to its reputation requiring an immediate response.

GENERAL GUIDELINES

During an emergency, the facility's incident management team will utilize various communication methods to effectively communicate with staff, patients, contractors and other entities, external partners, and any volunteers. This plan includes primary and alternate communication methods for all applicable parties. This plan also designates methods for the HIPPA compliant release of patient information when an emergency has rendered the facility inoperable and communicating any resource needs or availability of the facility. This plan must be reviewed and updated annually.

POLICY

The emergency communication efforts will be directed by the insert responsible person/entity. In his/her absence, the highest level available person in the health center chain of authority will assume this responsibility (e.g., Chief Operating Officer).

1. The insert responsible person/entity will appoint an insert responsible person/entity and an alternate, in writing, to direct and maintain the emergency communication efforts.
2. On an annual basis, all staff will provide and update their personal emergency contact information. Emergency contact information shall be kept confidential and used only for emergency contact situations. A master emergency contact list will be established and maintained by insert responsible person/entity (e.g., HR) and shared among senior leadership. This emergency contact list will be sorted by functional groups and specific personnel will serve as Emergency Group leaders. These leaders will be assigned to conduct and coordinate contact efforts for their specific group.
3. All media inquiries shall be directed to the health center's Public Information Officer. The insert name of person identified in number 1 of this list or designee shall provide information to the media only when authorized by senior leadership.
4. The primary method of communication for the health center shall be the health center's emergency notification system. This is an automated notification system that uses group email and telephone to communicate. In the event of a power outage at the receiver end, this system will be disabled and alternate methods of communication used. (insert your health center's process)

PROCEDURES

STAFF COMMUNICATIONS

- The primary forms of communication used to notify staff of an emergency will be:
  <Insert primary forms of communication/types of information that can/will be shared>
- In the event of failure or inoperability of primary communication methods, the organization will utilize the following alternative methods to notify staff:
  <Insert primary forms of communication/types of information that can/will be shared>
  - An updated list of staff primary and emergency contact information can be found:
    <Insert location/source/process here>

PATIENT COMMUNICATIONS

- The primary forms of communication used to notify patients of an emergency will be:
  <Insert primary forms of communication/types of information that can/will be shared>
- In the event of failure or inoperability of primary communication methods, the organization will utilize the following alternative methods to notify patients:
  <Insert primary forms of communication methods/types of information that can/will be shared>
  - An updated list of patient primary and emergency contact information can be found:
    <Insert location/source/process here>

EXTERNAL PARTNER COMMUNICATIONS

- The primary forms of communication used to notify external partners of an emergency will be:
  <Insert primary forms of communication/types of information that can/will be shared>

- In the event of failure or inoperability of primary communication methods, the organization will utilize the following alternative methods to notify external partner:
  <Insert primary forms of communication/types of information that can/will be shared>
- All external partner communications will be authorized by the <Insert title>, Incident Commander, or designee.

PUBLIC INFORMATION

- During an emergency, all public information activities shall be by the <Insert title>, Incident Commander, or designee, and coordinated by the health center's Public Information Officer (PIO).
- Communications Testing
- All communication methods should be routinely tested and verified for operability and connectivity. Any alternative methods used must be verified for connectivity.
  <Insert communications testing schedule/process>

SPECIAL CONSIDERATIONS

1. Identify and keep active records of employees that can speak and/or understand languages other than English.
2. Identify and keep active records of employees that are trained American Sign Language interpreters.
3. Keep track of hearing-aid compatible communications devices and put them in inventory or other easily-accessible areas.
4. Local 911 shall have personnel whom can communicate with people with access and functional needs (e.g., different languages, individuals with communication disabilities).
5. <Insert any other facility specific special considerations>

APPENDIX I ⟩ RISK COMMUNICATIONS

In all phases of a disaster, up-to-date and factual information is essential to preserve the health and well-being of individuals and organizations. In an effort to build trust and credibility, the Centers for Disease Control and Prevention (CDC) developed guidelines for Crisis and Emergency Risk Communications (CERC). The CERC guidelines assist health communicators, emergency responders, and leaders of organizations communicate effectively during emergencies. In the event of a pandemic, CERC identifies six principles your organization can follow to ensure you provide your staff and patients with information to make the right decisions.

Principle 1: BE FIRST

Crises are time sensitive. Quickly sharing information about a disaster can reduce the impacts on life and safety. In the beginning of an emergency rumors may begin to spread so it is important to share available facts to help curtail those rumors. Often the first source of information becomes the preferred source of information for the public.

Principle 2: BE RIGHT

Credibility is established by providing accurate information. Maintain as much transparency as possible when discussing the situation. Include what is known, what is not known, and what is being done to fill the gaps. Ensure that your health center's messages are backed up by emergency officials. Utilize subject-matter experts to check your facts. Incorrect information is worse than no information and incorrect information invalidates credibility.

Principle 3: BE CREDIBLE

Credibility is earned. Honesty and truthfulness should never be compromised, especially during a time of crisis. Acknowledge when you do not have an answer to a question and then work with experts to find an answer. Refrain from promising anything that is not certain, including injuries and fatalities, etc. Always refer to medical professionals on medical questions.

Principle 4: EXPRESS EMPATHY

Emergencies can cause uncertainty and helplessness. Fear of the unknown can disrupt daily lives. It is important to acknowledge fear and suffering. Addressing what people are feeling and their challenges gives them confidence in your organization. Empathy builds trust and rapport which will positively affect how open people are to receiving recommendations.

Principle 5: PROMOTE ACTION

During an emergency, giving people actionable ways to help mitigate the impacts is essential. This promotes a sense of control among individuals and organizations. Keep messages short and simple, like "turn around, don't drown" or "stay inside to survive." Simple actionable messages will go a long way in calming anxiety.

Principle 6: SHOW RESPECT

In times of crisis, people tend to feel vulnerable. When reporting important information, respectful communication promotes cooperation and rapport. Belief and practices regarding emergencies differ between cultures. It is important to actively listen to concerns and adapt behaviors and communications to promote understanding. Acknowledge and listen to fears and concerns. Actively engage and ask questions.

Note: When developing and communicating messaging, it is important to remember that individuals receive information in different ways. Offer alternate methods of communication such as use of a qualified American Sign Language interpreter or closed captioning. Provide translation services for those with limited English proficiency. Use simple and easy to understand language and avoid jargon. Provide redundant communication on different platforms for those with varying access to information such as television, radio, and social media.

APPENDIX J ⟩ MITIGATION PLAN

PURPOSE

This Mitigation Plan includes information on what steps that <Insert health center name> has taken to address issues identified in the annual risk assessment.

GENERAL GUIDELINES

Mitigation is the effort to reduce loss of life and property by lessening the impact of disasters. In order for mitigation to be effective we need to take action now—before the next disaster—to reduce human and financial consequences later (analyzing risk, reducing risk, and insuring against risk). It is important to know that disasters can happen at any time and any place and if we are not prepared, consequences can be fatal.

It must be understood that the role of mitigation will not completely remove the risk, but it is designed to lessen the impacts it can have to a facility and its staff and patients.

MITIGATION

- Mitigation Measures

1. <Insert title> will undertake an annual risk assessment by conducting a Hazard Vulnerability Assessment (HVA) and hazard mitigation activities. The purpose is to lessen the severity and impact of a potential emergency by identifying potential hazards that may affect the health center.
2. The full HVA would be a separate document. For detailed and in-depth results and mitigation strategies for the identified risks, see that document. In the table below, the top five threats/hazards have been identified in the most recent HVA. The top risks and mitigation steps to address those risks are:

RANK	THREAT/HAZARD	TYPE	RISK %	MITIGATION STEPS
1	[**Example** – Pandemic]	Natural	78%	Identified alternate care sites Created surge capacity plan Obtained 55 portable HEPA Units Created PPE cache for infectious disease for an additional 6-8 weeks of PPE
2				
3				
4				
5				

- **Preparedness Activities**

1. Staff are trained on and required to follow any instructions provided in an emergency notification. Staff may be notified through backup communications systems.
2. Staff are required to know the health center exit routes and assembly points.
3. <Insert health center name> will identify and clearly post evacuation route maps throughout the facility. Evacuation routes shall be marked on maps and floor plans and posted throughout the health center.
4. Staff are required to know the shelter-in-place procedures in the event a shelter-in-place is ordered.
5. Staff will be on alert to receive information from management staff or the Incident Commander. Be prepared to inform and advise patients, staff, and visitors at the health center of the possible impacts of an emergency, and what precautions may be necessary in order to ensure the safety of all persons within the health center.
6. Staff are required to know communication procedures and incident command structure to ensure clear communication and chain of command.
7. Staff are required to know the exit routes and safe evacuation procedures in the event an evacuation is ordered.
8. Emergency numbers shall be posted next to all phones with directives of whom and how to place calls and what information to provide.

<Insert other training activity/process here>

APPENDIX K ⟩ STAFF TRAINING AND EXERCISE PLAN

PURPOSE

This Training and Exercise Plan includes information on what steps that <Insert health center name> has taken to provide training to staff a as it relates to emergency operations and business continuity.

GENERAL GUIDELINES

A training and testing program is a cyclical process that begins with developing/updating your health center's Hazard Vulnerability Assessment (HVA) and writing, reviewing, and/or revising your policy and procedures to support your Emergency Operations Plan. You will use exercises as a means of "testing" to ensure your plans, policies, and procedures function as intended. Utilizing an all-hazards approach will allow you to focus on your capacities and capabilities to prepare for a broad range of events/disasters. This will enable you to tailor specific details to your health center, staff, and patient needs.

After testing you will complete the cycle by updating and/or revising you plans, policies, and procedures based on the lessons learned. Once you have completed this cycle you will start the process again by updating your HVA.

TRAINING AND EXERCISE PLAN (TEP)

- Required Training

1. Staff are trained on and required to follow any instructions provided in an emergency notification. Staff may be notified through backup communications systems.
2. Staff are required to know the facility exit routes and assembly points.
3. <Insert health center name> will identify and clearly post evacuation route maps throughout the facility. Evacuation routes shall be marked on maps and floor plans and posted throughout the health center.
4. Staff are required to know the shelter-in-place procedures in the event a shelter-in-place is ordered.
5. Staff will be on alert to receive information from management staff or the Incident Commander. Be prepared to inform and advise patients, staff, and visitors at the health center of the possible impacts of an emergency, and what precautions may be necessary in order to ensure the safety of all persons within the health center.
6. Staff are required to know communication procedures and incident command structure to ensure clear communication and chain of command.
7. Staff are required to know the exit routes and safe evacuation procedures in the event an evacuation is ordered.
8. Emergency numbers shall be posted next to all phones with directives of whom and how to place calls and what information to provide.
9. Core competency training is recommended for staff in accordance with their planned roles and responsibilities. This is as outlined in the table on the next page.

RECOMMENDED CORE COMPETENCIES FOR ALL HAZARD TYPES	
Basic	• Knowledge of how to activate the health center's emergency response plan • Understand the health center's security and scene control procedures for the basic level trained personnel • Knowledge of basic hazard and risk assessment techniques • Knowledge of how to select, use, inspect, and properly maintain the personal protective equipment used by basic level personnel • Knowledge of resources required to assist persons with access and functional needs
Mid level	• Knowledge and ability to demonstrate the competencies of basic level personnel • Knowledge of the basic hazard and risk assessment techniques • Understand how to select and use personal protective equipment provided to the mid-level trained personnel • Knowledge of relevant standard operational and termination procedures • Ability to perform basic control, containment, and/or confinement operations within the capabilities of the resources and personal protective equipment available • Knowledge of how to implement the Incident Command System • Knowledge of how to establish communications with outside agency command centers
Advanced	• Knowledge and ability to demonstrate the competencies from mid level • Ability to function within an assigned role in the Incident Management Structure • Understand hazard and risk assessment techniques • Ability to perform advanced control, containment, and/or confinement operations within the capabilities of the resources and personal protective equipment available

<Insert other training activity/process here>

1. In addition, <Insert health center name> senior leadership, department directors, managers, supervisors, and others that might assume an emergency response leadership role, will receive education consistent with the National Incident Management System (NIMS) requirements (Incident Command System courses 100, 200 & 700) and jurisdictionally-specific emergency response. The types of NIMS training are listed in the table below:

NATIONAL INCIDENT MANAGEMENT SYSTEM (NIMS) COMPLIANCE TRAINING	
STAFF ROLE	**NIMS BASED TRAINING**
Personnel likely to be involved as initial responders	• ICS-100: Introduction to ICS or equivalent • FEMA IS-700: NIMS or equivalent
Personnel likely to function as unit/care area supervisors or specialists	• ICS-100: Introduction to ICS or equivalent • ICS-200: Basic ICS or equivalent • FEMA IS-700: NIMS or equivalent
Personnel likely to function as managers, unit leaders, or branch directors	• ICS-100: Introduction to ICS or equivalent • ICS-200: Basic ICS or equivalent • FEMA IS-700: NIMS or equivalent
Personnel identified with primary disaster management, policy response and creation*	• ICS-100: Introduction to ICS or equivalent • ICS-200: Basic ICS or equivalent • FEMA IS-700: NIMS or equivalent • FEMA IS-800.A: National Response Plan Framework (NRP), An Introduction* * NOTE: Personnel whose primary responsibility is in emergency management must complete this training.

- **Drills and Exercises**

1. <Insert health center name> participates in or conducts and documents annual training and test plans with two exercises annually:

   a. **Training:** Conduct and document initial and annual training on your emergency preparedness policies and procedures for all staff

   b. **Exercises:** Must conduct and document two exercises annually:
      - A community-based full-scale exercise
      - A second full-scale or tabletop exercise

2. Exercises can be in many forms, including:

   a. **Discussion-based exercises** include seminars, workshops, tabletop exercises (TTXs), and games. These types of exercises can be used to familiarize players with, or develop new, plans, policies, agreements, and procedures. Discussion-based exercises focus on strategic, policy-oriented issues. Facilitators and/or presenters usually lead the discussion, keeping participants on track towards meeting exercise objectives.

b. **Seminars** generally orient participants to, or provide an overview of, authorities, strategies, plans, policies, procedures, protocols, resources, concepts, and ideas. As a discussion-based exercise, seminars can be valuable for entities that are developing or making major changes to existing plans or procedures. Seminars can be similarly helpful when attempting to assess or gain awareness of the capabilities of interagency or inter-jurisdictional operations. Goals of a seminar exercise are:
   - ○ Orientate participants to new or existing plans, policies, or procedures.
   - ○ Research or assess interagency capabilities or inter-jurisdictional operations.
   - ○ Construct a common framework of understanding.

c. **Workshops**, although similar to seminars, differ in two important aspects: participant interaction is increased, and the focus is placed on achieving or building a product. Effective workshops entail the broadest attendance by relevant stakeholders. Products produced from a workshop can include new standard operating procedures (SOPs), emergency operations plan, continuity of operations plans, or mutual aid agreements. To be effective, workshops should have clearly defined objectives, products, or goals, and should focus on a specific issue. Goals for a workshop may include:
   - ○ Develop new ideas, processes, or procedures.
   - ○ Develop a written product as a group in coordinated activities.
   - ○ Obtain consensus.
   - ○ Collect or share information.

d. T**abletop exercise (TTX)** are intended to generate discussion of various issues regarding a hypothetical, simulated emergency. TTXs can be used to enhance general awareness, validate plans and procedures, rehearse concepts, and/or assess the types of systems needed to guide the prevention of, protection from, mitigation of, response to, and recovery from a defined incident. Generally, TTXs are aimed at facilitating conceptual understanding, identifying strengths and areas for improvement, and/or achieving changes in perceptions. During a TTX, players are encouraged to discuss issues in depth, collaboratively examining areas of concern and solving problems. The effectiveness of a TTX is derived from the energetic involvement of participants and their assessment of recommended revisions to current policies, procedures, and plans. TTXs can range from basic to complex. In a basic TTX the scenario is presented and remains constant—it describes an event/disaster and exercise participants discuss the situation at hand based on their training, plans, and policies. A facilitator usually introduces and updates the original event/disaster by adding a new event or circumstance. Players discuss the issues raised by each problem, referencing existing plans, policies, and procedures for direction. Goals for a tabletop exercise may include:
   - ○ Identify strengths and shortfalls
   - ○ Enhance understanding of new concepts
   - ○ Seek to change existing attitudes and perspectives

e. **A functional exercise (FE)** is designed to validate and evaluate capabilities, and multiple functions. FEs focus on exercising plans, policies, procedures, and staff members are involved in management, direction, command, and control functions. In FEs, events are created using an exercise scenario with scenario updates that drive your actions to complete the tasks needed to meet the objectives. An FE is conducted in a realistic, real-time environment; however movement of personnel and equipment is usually simulated. FE controllers typically use a Master Scenario Events List (MSEL) to ensure participant activity remains within limits and ensure exercise objectives are accomplished. FEs involve multiple functions and use simulated deployment of resources and personnel.

f. **A full scale exercise (FSE)** is typically the most complex and resource-intensive type of exercise. They involve multiple entities and will serve to validate your ability to respond to an event/ disaster preparedness. FSEs often include many players working within the Incident Command System (ICS). In an FSE, events are created using an exercise scenario. Updates that drive activity at the operational level are feed into the scenario at specific times to create objectives to be accomplished. FSEs are usually conducted in a real-time, stressful environment that is intended to mirror a real incident. Personnel and resources may be mobilized and deployed to the scene. FSEs are intended to serve as an exercise program management and communications tool, which informs stakeholders and guides the development of future trainings and exercises.

3. Exercise Document Requirements

a. **Exercise Plan (ExPlan):** The Exercise Plan gives stakeholders, observers, media personnel, and players from participating organizations information they need to observe or participate in the exercise. Some exercise material is intended for the exclusive use of exercise planners, controllers, and evaluators, but players may view other materials that are necessary to their performance. All exercise participants may view the ExPlan.

b. **Master Sequence of Events List (MSEL):** For running the exercise, the MSEL documents the trigger/activation points to stimulate response from the participants.

c. **Exercise Evaluation Guides (EEGs):** Evaluation of your drill or exercise will help measures performance against the exercise objectives that were created while planning the exercise. The evaluations will help gather observations and feedback collected during the exercise. This will help identify and document strengths and areas for improvement.

d. **After Action Report (AAR) and Improvement Plan (IP):** The After-Action Report (AAR) and Improvement Plan (IP) summarizes the relevant and key information captured about the exercise and makes recommendations for improvements that can be made to training, policies, and procedures.

APPENDIX L 〉BUSINESS INTERRUPTION INSURANCE

Business interruption insurance helps replace lost income and pay for extra expenses when a business is affected by a covered peril. Business interruption coverage is typically part of a business owners insurance policy.

Business interruption insurance helps protect against lost income after a covered peril affects a business. Covered perils typically include theft, fire, wind, falling objects or lightning.

If a covered loss forces your business to shut down, your interruption insurance can help cover your operating expenses, like:

- Revenue you would normally make if your business were open.
- Mortgage, rent, and lease payments for the space your business operates from.
- Loan payments that you need to make during that time.
- Taxes, whether you pay them monthly or quarterly.
- Payroll for your employees.
- Relocation costs you must move to a new or temporary location because of physical damages.
- Extra expenses if, for example, you need to rent another space to temporarily run your business after a covered loss.
- Training costs for employees to learn how to use new machinery or equipment after a covered loss.

For example, if a fire damages your business, leaving the building uninhabitable and destroying equipment, business interruption coverage may help reimburse you in two ways:

1. For lost income from the destroyed equipment, and
2. For extra expenses if you must temporarily relocate your business because of the fire (for example, the cost of rent at the temporary location).

Many insurance agencies offer business interruption insurance. Contact your insurance provider for details.[1]

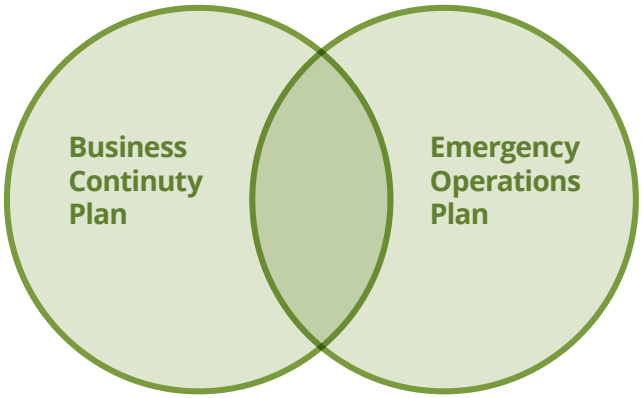
[1] The Hartford. (n.d.). Business Interruption Insurance.
Retrieved from Thehartford.com: https://www.thehartford.com/business-insurance/business-interruption-insurance

APPENDIX M ⟩ BUSINESS CONTINUITY PLAN vs EMERGENCY OPERATIONS PLAN

When responding to an incident, a health center will need to activate two different plans:

- **Emergency Operations Plan**
- **Business Continuity Plan**

These plans will be activated simultaneously as they work together during a response. Emergency response and emergency operations plans focus on the safety and protection of life, assets, and the environment. On the other hand, business continuity focuses on continuing the operations of the health center until it can return to normal. The differences between the plans and how and when they are implemented are discussed in detail below.



EMERGENCY OPERATIONS PLAN

Emergency operations plans (EOP) are developed for coordinating health centers' response to specific types of incidents. The plans and responses are tactical in nature, in that most of the incidents will last a short period of time and are brought under control rather quickly. A more serious incident may require a response from health centers which can last two or three days and may involve outside agencies such as local fire and police. The emergency operations plan takes into consideration these possibilities and address the incident and the period immediately after the incident in order to return critical health center operations to a minimum level.

An emergency operations plan provides the structure and processes that the health center utilizes to respond to and initially recover from an event. The hallmark of an EOP is the activation of the incident management structure and incident management teams (see below). Emergency response planning asks, "in an emergency, what needs to get done and how?" Considerations that go into this question include:

- Who is in charge?
- What is the communication/coordination pathways and who needs to be included?
- What activities need to happen to respond to the emergency?
- How will those activities be resourced (staff, equipment, money)?

BUSINESS CONTINUITY PLAN

Business continuity plans on the other hand are strategic in nature and are concerned with returning the health center to full normal operations as soon as possible after an incident. This type of plan addresses the aftermath of a critical incident and ensures the health center can continue to operate and sustain long term recovery. The plan must address the loss of productivity and any physical damage resulting from an incident while normal services and operations are being restored. While departments such as Facilities, Safety, and Operations components will normally be the lead departments in a critical incident response, Finance, Programs,

Risk Management, Public Relations, and Information Services are the health center departments most often responsible for carrying out the aspects of the Business Continuity plan.

Business continuity planning asks, "how do we keep our health center running and what is the bare minimum on which we'd be able to do it?" Considerations that go into this include:

- What are the essential functions of our health center?
- What is the minimum number of staff that could sustain those functions in a crisis?
- Who is in charge and who should be assigned to cover for them if they are unable to fill their role in a crisis?
- Can we function without a physical office/location? If not, do we have a backup location? If so, are staff adequately equipped for remote work?
- What systems/equipment, supplies, and records/databases do we have and what is our plan for protecting/accessing them during a crisis?

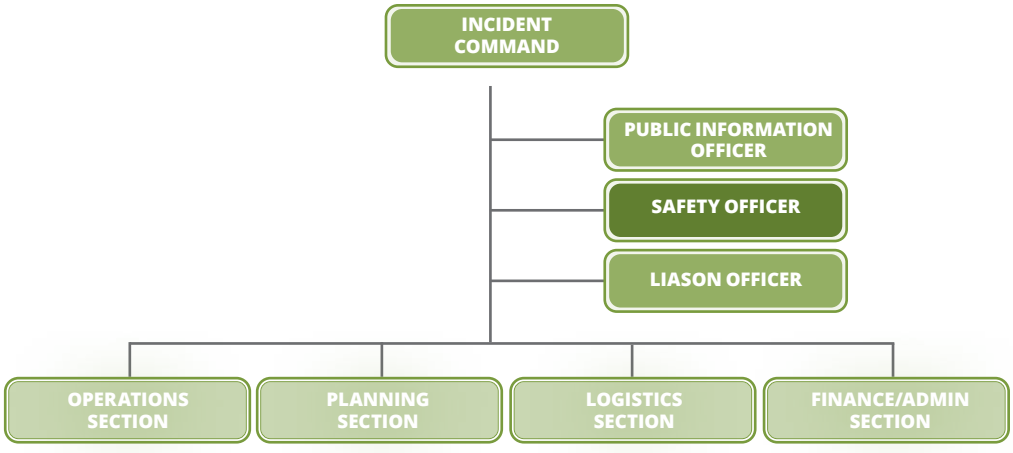
INCIDENT RESPONSE

The Incident Command System (ICS) is designed to manage any size of incident from the response phase through the recovery phase. The structure of ICS is designed to be scalable according to the severity and nature of the event, as well as, to meet the changing conditions and demands of the incident. The incident command structure allows organizations to respond to any emergency in a planned, organized, and efficient way. ICS is used widely in both the public and private sector to manage incidents and is the worldwide emergency management standard. For more information on ICS, please see the information below and further information in our resource section.

INCIDENT MANAGEMENT TEAM

The purpose of the Incident Management Team (IMT) is to organize and coordinate all aspects of response and recovery efforts following an incident. The IMT is divided into sections according to four functional areas: operations, planning, logistics, and finance/admin. The IMT also includes additional staff that fill supporting roles in public information, safety, and interagency coordination.

INCIDENT MANAGEMENT TEAM (IMT) COMMAND STRUCTURE



INCIDENT COMMAND ROLES AND RESPONSIBILITIES

Incident Commander

The Incident Commander (IC) is responsible for the overall management of the incident. The IC establishes the strategy and tactics for the incident response effort and has the ultimate responsibility for the success of all response and recovery activities. The IC role is filled at every incident, no matter how small or large and is selected by qualifications, experience, and level of authority within the organization. In collaboration with Section Chiefs, the IC determines incident objective and strategy, sets immediate priorities, and authorizes an Incident Action Plan.

Public Information Officer

The Public Information Officer (PIO) reports to the Incident Commander and is responsible for the development and release of information about the incident. The PIO conducts media briefings, develops messaging, distributes information to incident personnel, and works closely with other members of the IMT.

Safety Officer

The Safety Officer is responsible for monitoring and assessing hazardous and unsafe situations as well as developing measures for assuring personal safety. The Safety Officer reports directly to the IC and is the only person that can supersede the IC in the event of an unsafe situation.

Liaison Officer

The Liaison Officer's (LO) role is to serve as the point of contact for assisting and coordinating activities between the Incident Commander and other healthcare providers and government agencies. The LO reports directly to the Incident Commander.

Operations Section Chief

The Operations Section Chief manages the incident's tactical operations by directly supervising all resources assigned to the Operations Section. The function of the Operations Section is to accomplish the response and recovery strategies by directing resources to execute tactical objectives. The Operations Section Chief directs all the incident tactical operations and assists the IMT in the development of the Incident Action Plan (IAP).

Planning Section Chief

The Planning Section Chief supervises the collection, evaluation, processing, and dissemination of the Incident Action Plan (IAP). The function of the Planning Section is to collect and evaluate information that is needed for preparation of the IAP. The Planning Section forecasts the probable course of events the incident may take and prepares alternative strategies for changes in or modifications to the IAP.

Logistics Section Chief

The Logistics Section Chief manages logistical needs and provides facilities, services, people, and materials in support of the incident. The Logistics Section is responsible for all service support requirements needed to facilitate effective and efficient incident management, including ordering resources from off-incident locations. This Section also provides facilities, security, transportation, supplies, equipment maintenance and fuel, food services, and communications and information technology support.

Finance/Administrative Section Chief

The Finance/Administration Section Chief is responsible for all financial, administrative, and cost analysis aspects of an incident. The Finance/Administration Section must fiscally manage the incident, including claims processing, contracting, and administrative functions.

APPENDIX N ⟩ EQUIPMENT INFORMATION INVENTORY

EQUIPMENT	SERIAL NUMBER/ KEY/ LICENSE	COMPANY	WARRANTY EXPIRATION DATE	SERVICE CONTRACT – VENDOR INFORMATION

APPENDIX O ⟩ TRANSITION SCHEDULE TEMPLATE

TRANSITION SCHEDULE				
Business Continuity Team	Team Lead Name 1 Name 2 (alternate)		Team Members Martha Stewart Name 2 Name 3 Name 4	
Senior Leadership Sign-off on Final Business Continuity Plan	Date June 1, 2021			
BC Plan Team Meetings Schedule	Date 1 6/12/21	Date 2 6/26/21	Date 3	Date 4
	Topic Training of BC	Topic Develop Exercise	Topic	Topic
BC Plan Staff Training Schedule	Date 1 6/12/21	Date 2	Date 3	Date 4
	Topic Overview of BC	Topic	Topic	Topic
BC Plan Drill & Exercise Schedule	Date 1 8/1/21	Date 2	Date 3	Date 4
	Topic Power Outage	Topic	Topic	Topic

APPENDIX P ⟩ ALTERNATE LOCATION SUPPLIES CHECKLIST

Insert additional supplies as needed.

RESOURCE	QTY AVAIL	HR QTY	SUPPLIER	ALTERNATE SUPPLIER
Medical Supplies				
Oxygen				
BLS Supplies				
ALS Supplies				
Band-Aids				
Gowns				
Masks				
Hand sanitizer				
Diagnostic Supplies				
Thermometers				
Stethoscopes				
Glucometers				
Water (# of cases)				
Food				
Canned				
Other				
Medical Equipment				
Beds				
Linens (sheets, pillows, pillow cases, hand towels, bath towels)				
Evacuation Sleds				
Evacuation Chairs				
Wheelchairs				
IV poles				
Pharmacy carts				
AED				
Staff Support				
Spare Scrubs				
Cots/Linen				
Comfort Kits				
MRE's				
Chairs (correlation with staffing level)				
Desks (correlation with staffing level)				

RESOURCE	QTY AVAIL	HR QTY	SUPPLIER	ALTERNATE SUPPLIER
Facility Support				
Flashlights				
Sandbags				
Duct Tape				
Portable Lights				
Portable Fans				
Communications Support				
Fax machine				
Email access				
Telephones				
Portable Radios				
Other				
Refrigerators (food, meds)				
Toilet paper				
Paper towels				
Administrative Supplies				
Pens				
Stapler				
Staples				
Tape				
Paper clips				
Chart holder/Clip boards				
File folders				
Batteries				
White board				
Dry-erase markers				
Trashcans and liners				
Lamps				
Light bulbs				
Paper				
Filing cabinet				
Sign-in/Sign-out forms				
Pre-printed order forms				
Blank physician order forms				
Nursing flow sheets				

APPENDIX Q ⟩ KEY CONTACTS, VENDORS, AND SUPPLIERS

Management Contact List

POSITION	NAME	PRIMARY AND SECONDARY PHONE	EMAIL
Executive Director ICS Role:	<Insert name>	<Insert phone numbers>	<Insert email>
Safety Director ICS Role:	<Insert name>	<Insert phone numbers>	<Insert email>
Medical Director ICS Role:	<Insert name>	<Insert phone numbers>	<Insert email>
Operations Director ICS Role:	<Insert name>	<Insert phone numbers>	<Insert email>
Finance Director ICS Role:	<Insert name>	<Insert phone numbers>	<Insert email>
Human Resources Director ICS Role:	<Insert name>	<Insert phone numbers>	<Insert email>
<Insert Position>	<Insert name>	<Insert phone numbers>	<Insert email>
<Insert Position>	<Insert name>	<Insert phone numbers>	<Insert email>
<Insert Position>	<Insert name>	<Insert phone numbers>	<Insert email>

Outside Agency/Vendor Contact List

AGENCY	CONTACT NAME/TITLE	PRIMARY AND SECONDARY PHONE	EMAIL
Fire – Business Line Agency:			
Fire – Emergency			
EMS – Emergency			
Law Enforcement Office Business Line			
Law Enforcement Emergency			
Coroner			
(City/County/State) Office of Emergency Management (OEM)			
OEM Public Information Officer (PIO)			
OEM Point of Contact			
County Health Department Emergency Operations Center (EOC)			
EOC Public Information Officer (PIO)			
EOC Point of Contact			
Infectious Disease Agency			
Hospital			
UTILITIES			
Utilities-Water			
Utilities-Electric			
Utilities-Heating Oil			
Utilities-Gas (Propane or Natural)			
Generator Fuel (Gas, Propane, Diesel)			
IT Support (if external)			
VENDORS			
Food			
Water (beyond utilities)			
Pharmaceuticals			
Medical Supplies			
Medical Equipment			
Janitorial			

List of Approved Employees Who Speak Another Language

NAME	LANGUAGE(S)	SIGN LANGUAGE?	CELL PHONE CONTACT
<Insert Name>	<Insert language(s)>	<Yes> <No>	<Insert phone number>
<Insert Name>	<Insert language(s)>	<Yes> <No>	<Insert phone number>
<Insert Name>	<Insert language(s)>	<Yes> <No>	<Insert phone number>
<Insert Name>	<Insert language(s)>	<Yes> <No>	<Insert phone number>
<Insert Name>	<Insert language(s)>	<Yes> <No>	<Insert phone number>
<Insert Name>	<Insert language(s)>	<Yes> <No>	<Insert phone number>

APPENDIX R ⟩ CASH PROJECTIONS

Successful business continuity planning must include cash flow management. This is a critical for any business, large or small, as cash is the lifeblood of any business, especially in a crisis. Effective cash management includes the following:

- Frequently analyzing a company's working capital requirements
- Optimizing cash flows and funding sources while looking for opportunities to defer payments
- Creating timely cash flow projections while looking for ways to reduce variable costs
- Considering alternative or non-traditional revenue streams
- Getting clarity on available credit options
- Holding off on tax payments until late summer
- Taking advantage of government relief efforts including tax deferrals

Most disasters or emergencies do not last forever, but you should plan in a way that enables your health center to remain open indefinitely during these times.

EXAMPLE Work Sheet

CASH BALANCE	January	February	March	April
Opening Cash Balance	$1,000.00	$1,100.00	($300.00)	($300.00)
REVENUES				
In-store Sales	$500	$200		
Online Sales	$150	$100		
Other Reveues	$200			
Total Revenues	$850	$300	$0	$0
GROSS PROFITS				
Cost of goods sold	$40			
Gross Profits	$810	$300	$0	$0
Gross Profit Margins	95.30%	100%	-	-
EXPENSES				
Fixed Costs				
Rent	$500			
Insurance				
Fees (banking, licenses, etc.)				
Total Fixed Costs	$500	$0	$0	$0
Variable Costs				
Payroll	$200	$200		
Shipping Costs		$500		
Utilities		$10		
Total Variable Costs	$200	$710	$0	$0

APPENDIX S ⟩ MUTUAL AID MEMORANDUM OF UNDERSTANDING (MOU)

The MOU template document was adapted from the Hospital Surge Capacity Toolkit created by the National Association of City and County Health Official's Advanced Practice Center. To view the complete toolkit, please visit: Hospital Surge Capacity Toolkit. The model language can provide a framework for a response discussion between healthcare organizations and local disaster planners or with fellow healthcare organizations.

<Insert effective dates here>

INTRODUCTION AND BACKGROUND

Health care providers are susceptible to both natural and man-made to disasters that could exceed the resources of any individual organization. A disaster could result from incidents generating an overwhelming number of patients, from a smaller number of patients whose specialized medical requirements exceed the resources of the impacted facility (e.g., hazmat injuries, pulmonary, trauma surgery, etc.), or from incidents such as building problems resulting in the need for partial or complete evacuation.

PURPOSE OF MUTUAL AID MEMORANDUM OF UNDERSTANDING

The mutual aid support concept is well established and is considered to be the "standard of care" in most emergency response disciplines. The purpose of this mutual aid support agreement is to aid healthcare organizations in their emergency management response by creating a Mutual Aid System (MAS). MAS addresses the loan of medical personnel, pharmaceuticals, supplies, and equipment, or assistance with emergent evacuation, including accepting transferred patients.

This Mutual Aid Memorandum of Understanding (MOU) is a voluntary agreement among the undersigned healthcare organizations for the purpose of providing mutual aid at the time of a medical disaster. For purposes of this MOU, a disaster is defined as an overwhelming incident that exceeds the effective response capability of the impacted health care facility or facilities. An incident of this magnitude will almost always involve the local emergency management agency and the Jurisdiction Public Health Department. The disaster may be an "external" or "internal" event for a healthcare organization and it is assumed for the purposes of this MOU that each affected healthcare organization's emergency management response plans have been fully implemented.

This document addresses the relationships between and among healthcare organizations and is intended to augment, not replace, each facility's disaster plan. The MOU also provides the framework for participating healthcare organizations to coordinate as a single HEALTHCARE ORGANIZATION-MAS community in actions with Jurisdiction Public Health Department, and Jurisdiction Emergency Medical Services (EMS) during planning and response. This document does not replace but rather supplements the rules and procedures governing interaction with other organizations during a disaster (e.g., law enforcement agencies, EMS, Public Health Department, fire departments, American Red Cross, etc.).

By signing this Memorandum of Understanding, each healthcare organization is evidencing its intent to abide by the terms of the MOU in the event of a medical disaster as described above. The terms of this MOU are to be incorporated into each of the healthcare organization's emergency management plans.

DEFINITION OF TERMS

Donor MOU Partner	The healthcare organization that provides personnel, pharmaceuticals, supplies, or equipment to a facility experiencing a medical disaster.
Donor-Receiving MOU Partner	The healthcare organization that receives transferred patients from a facility responding to a disaster. When personnel or materials are involved, the providing healthcare organization is referred to as the donor healthcare organization.
Impacted MOU Partner	The healthcare organization where the disaster occurred or where disaster victims are being treated. Referred to as the Impacted MOU Partner when pharmaceuticals, supplies, or equipment are requested or, as the patient-transferring healthcare organizations when the evacuation of patients is required.
Incident Command Center (ICC)	An area established in a healthcare organization during an emergency that is the facility's primary source of administrative authority and decision-making.
Jurisdiction DOC/EOC (Jurisdiction Department of Public Health, Department Operations Center)	A communication and information center that has MAS network capabilities allowing for the immediate determination of available healthcare organizations resources at the time of a disaster. The Jurisdiction DOC/EOC does not have any decision-making or supervisory authority and merely collects and disseminates information.
MAS	Mutual Aid System
Medical Disaster	An incident that exceeds a facility's effective response capability or a situation that cannot be appropriately resolved solely by using the facility's own resources. Such disasters will very likely involve the local emergency management agency, Jurisdiction Emergency Management Agency, the Jurisdiction Public Health Department and may involve the mobilization of publicly owned response materials and equipment or the loan of medical and support personnel, pharmaceuticals, supplies, and equipment from another facility, or, the emergent evacuation of patients.
Participating healthcare organizations	Health care facilities that have fully committed to MAS and signed the healthcare organization Memorandum of Understanding.
Partner ("Buddy")	The designated facility that an Impacted healthcare organization communicates with as a facility's "first call for help" during a medical disaster (developed through an optional partnering arrangement). MOU Partner should meet at least twice a year to discuss contingency plans.
Recipient healthcare organization	The impacted facility. The healthcare organization where disaster patients are being treated and have requested personnel or materials from another facility.
Staff (or personnel)	Staff or personnel are employees of a specific healthcare organization.

GENERAL PRINCIPLES OF UNDERSTANDING

- **Participating Community Health Centers:** Each healthcare organization designates a representative to attend the Mutual Aid System meetings and coordinate the mutual aid initiatives with the individual HEALTHCARE ORGANIZATION's emergency management plans.
- **MOU Partner Concept:** Each HEALTHCARE ORGANIZATION has the option of linking to a designated partner or "buddy" HEALTHCARE ORGANIZATION as the HEALTHCARE ORGANIZATION of first call for help during a disaster. The HEALTHCARE ORGANIZATION comprising each partner-network should develop, prior to any medical disaster, methods for coordinating communication between themselves, responding to the media, and identifying the locations to enter their buddy HEALTHCARE ORGANIZATION's security perimeter.
- **Implementation of Mutual Aid System Memorandum of Understanding:** A healthcare organization facility becomes a participating HEALTHCARE ORGANIZATION when an authorized leadership signs the MAS MOU. During a medical emergency, only the authorized leadership (or designee) or HEALTHCARE ORGANIZATIONCC at each Community Health Center has the authority to request or offer assistance through HEALTHCARE ORGANIZATION-MAS. If the Jurisdiction DOC/EOC has been established, communications for assistance should go through the Jurisdiction DOC/EOC.
- **HEALTHCARE ORGANIZATION:** The impacted facility's emergency operations center is responsible for informing the Jurisdiction DOC/EOC of its situation and defining needs that cannot be accommodated by the HEALTHCARE ORGANIZATION itself or any existing partner HEALTHCARE ORGANIZATION. The senior leadership or designee is responsible for requesting personnel, pharmaceuticals, supplies, equipment, or authorizing the evacuation of patients. Logistics include identifying the number and specific location where personnel, pharmaceuticals, supplies, equipment, and estimated return date of borrowed supplies, etc.
- **Jurisdiction DOC/EOC:** Each HEALTHCARE ORGANIZATION will participate in an annual MAS exercise that includes communicating to the Jurisdiction DOC/EOC a set of data elements or indicators describing the HEALTHCARE ORGANIZATION's resource capacity. The Jurisdiction DOC/EOC will serve as an information center for recording and disseminating the type and amount of available resources at each HEALTHCARE ORGANIZATION. During a disaster drill or emergency, each HEALTHCARE ORGANIZATION will report to the Jurisdiction DOC/EOC the current status of their indicators.
- **Documentation:** During a disaster, the recipient HEALTHCARE ORGANIZATION will accept and honor the donor HEALTHCARE ORGANIZATION's standard requisition forms. Documentation (see attached Resource Accounting Records) should detail the items involved in the transaction, condition of the material prior to the loan (if applicable), and the party responsible for the material.
- **Authorization:** The recipient facility will have supervisory direction over the donor facility's staff, borrowed equipment, etc., once they are received by the recipient HEALTHCARE ORGANIZATION.
- **Financial & Legal Liability:** The recipient HEALTHCARE ORGANIZATION will assume legal responsibility for the personnel and equipment from the donor HEALTHCARE ORGANIZATION during the time the personnel, equipment and supplies are at the recipient HEALTHCARE ORGANIZATION. The recipient HEALTHCARE ORGANIZATION will reimburse the donor HEALTHCARE ORGANIZATION, to the extent permitted by federal law, for all of the donor HEALTHCARE ORGANIZATION's costs determined by the donor HEALTHCARE ORGANIZATION's regular rate or in the case of materials, at the fair market rate. Costs shall include all costs arising from the use, damage, loss, and return of borrowed materials.
- **Communications:** HEALTHCARE ORGANIZATIONs along with Jurisdiction Public Health Department will collaborate on maintaining a robust contact information matrix of telephone, email, satellite telephone, pager, and other communication pathways to ensure a reliable method to communicate with the Jurisdiction DOC/EOC and other HEALTHCARE ORGANIZATIONs
- **Emergency Management Committee Chairperson:** Each HEALTHCARE ORGANIZATION's Emergency Management Committee Chairperson is responsible for disseminating the information regarding this MOU to relevant HEALTHCARE ORGANIZATION personnel, coordinating and evaluating the HEALTHCARE ORGANIZATION's participation in exercises of the mutual aid system, and incorporating the MOU concepts into the HEALTHCARE ORGANIZATION's emergency management plan.

- **Hold Harmless Condition:** The recipient HEALTHCARE ORGANIZATION should hold harmless the donor HEALTHCARE ORGANIZATION for acts of negligence or omissions on the part of the donor HEALTHCARE ORGANIZATION in their good faith response for assistance during a disaster. The donor HEALTHCARE ORGANIZATION, however, is responsible for appropriate credentialing of personnel and for the safety and integrity of the equipment and supplies provided for use at the recipient HEALTHCARE ORGANIZATION.

GENERAL PRINCIPLES GOVERNING MEDICAL OPERATIONS, THE TRANSFER OF PHARMACEUTICALS, SUPPLIES, AND/OR EQUIPMENT

- **Partner HEALTHCARE ORGANIZATION concept:** Each HEALTHCARE ORGANIZATION has the option of designating a primary and secondary partner or *buddy HEALTHCARE ORGANIZATIONs, that may be contacted first when a HEALTHCARE ORGANIZATION needs to make a "first or second call for help". During a disaster, the impacted HEALTHCARE ORGANIZATION may first call its pre-arranged primary or secondary partner HEALTHCARE ORGANIZATION for personnel or material assistance. The partner HEALTHCARE ORGANIZATION will inform the impacted HEALTHCARE ORGANIZATION of the degree and time frame in which it can meet the request.*
- **Jurisdiction EOC:** The impacted HEALTHCARE ORGANIZATION is responsible for notifying and informing the Jurisdiction EOC of its personnel or material needs and the degree to which its partner HEALTHCARE ORGANIZATIONs are unable to meet these needs. Upon the request by the senior leadership or designee of the impacted HEALTHCARE ORGANIZATION, the Jurisdiction EOC will contact the other participating HEALTHCARE ORGANIZATIONS to determine the availability of additional personnel or material resources, as required by the situation. The impacted HEALTHCARE ORGANIZATION will be informed as to which HEALTHCARE ORGANIZATIONs should be contacted directly for assistance that has been offered. The senior leadership (or designee) of the impacted HEALTHCARE ORGANIZATION will coordinate directly with the senior leadership (or designee) of the potential donor HEALTHCARE ORGANIZATION for this assistance.
- **Initiation of transfer of personnel, and/or material resources:** Only the senior HEALTHCARE ORGANIZATION leadership or designee at each HEALTHCARE ORGANIZATION has the authority to initiate the transfer or receipt of personnel, or material resources. The senior leadership (or designee) and medical director, in conjunction with the directors of the affected services, will make a determination as to whether medical staff and other personnel from another facility will be required at the impacted HEALTHCARE ORGANIZATION to assist in patient care activities.

Personnel offered by donor HEALTHCARE ORGANIZATIONs should be limited to staff that are fully qualified, and licensed, accredited, or credentialed (if applicable) by the donor HEALTHCARE ORGANIZATION.

SPECIFIC PRINCIPLES OF UNDERSTANDING

1. Medical Operations/Loaning Personnel

a. **Communication of request:** The impacted HEALTHCARE ORGANIZATION's initial request for the transfer of personnel can be made verbally. However written documentation of the request should be received by the donor HEALTHCARE ORGANIZATION prior to the transfer of personnel to the recipient HEALTHCARE ORGANIZATION. The recipient HEALTHCARE ORGANIZATION will identify to the donor HEALTHCARE ORGANIZATION the following:

- ○ The type and number of requested personnel
- ○ An estimate of how quickly the requested personnel are needed
- ○ The location where personnel are to report and
- ○ An estimate of how long the personnel will be needed

b. **Documentation:** The arriving donated personnel will be required to present their donor HEALTHCARE ORGANIZATION identification badge and a copy of their professional license (if applicable) at the site designated by the recipient HEALTHCARE ORGANIZATION. The recipient HEALTHCARE ORGANIZATION will be responsible for the following:

- Confirming the donated personnel's ID badge, professional license and any accreditations or credentials (if applicable) using information contained in the list of personnel provided by the donor HEALTHCARE ORGANIZATION, and
- Providing additional identification, e.g., "visiting personnel" badge, to the arriving donated personnel.

The recipient HEALTHCARE ORGANIZATION will accept the professional credentialing determination of the donor HEALTHCARE ORGANIZATION but only for those services for which the personnel are credentialed at the donor HEALTHCARE ORGANIZATION.

c. **Supervision:** The recipient HEALTHCARE ORGANIZATION's senior leadership or designee identifies where and to whom the donated personnel are to report, and the professional staff of the recipient HEALTHCARE ORGANIZATION who will supervise the donated personnel. The supervisor or designee will meet the donated personnel at the point of entry of the facility and brief the donated personnel of the situation and their assignments. If appropriate, the "emergency staffing" rules of the recipient HEALTHCARE ORGANIZATION will govern the assigned shifts. The donated personnel's shift, however, should not be longer than the customary length practiced at the donor HEALTHCARE ORGANIZATION.

d. **Legal and financial liability:** Liability claims, malpractice claims, disability claims, attorneys' fees, and other incurred costs are the responsibility of the recipient HEALTHCARE ORGANIZATION. An extension of liability coverage will be provided by the recipient facility, to the extent permitted by federal law, insofar as the donated personnel are operating within their scope of practice. The recipient HEALTHCARE ORGANIZATION will reimburse the donor HEALTHCARE ORGANIZATION for the salaries of the donated personnel at the donated personnel's rate as established at the donor HEALTHCARE ORGANIZATION if the personnel are employees being paid by the donor HEALTHCARE ORGANIZATION. The reimbursement will be made within ninety days following receipt of the invoice.

The medical director of the recipient HEALTHCARE ORGANIZATION will be responsible for providing a mechanism for granting emergency credentials and or temporary privileges' for donor HEALTHCARE ORGANIZATION physicians. The HEALTHCARE ORGANIZATION's senior leadership will be responsible for providing a mechanism for granting emergency credentialing privileges for nurses and other licensed health care providers to provide services at the recipient HEALTHCARE ORGANIZATION.

e. **Demobilization procedures:** The recipient HEALTHCARE ORGANIZATION will provide and coordinate any necessary demobilization procedures and post-event stress debriefing. The recipient HEALTHCARE ORGANIZATION is responsible for providing the transportation necessary for donated personnel's return to the donor HEALTHCARE ORGANIZATION.

2. Transfer of Pharmaceuticals, Supplies or Equipment

a. **Communication of Request:** The impacted HEALTHCARE ORGANIZATION's initial request for the transfer of pharmaceuticals, supplies, or equipment (hereafter "materials") can be made verbally. However, written documentation of the request should be received by the donor HEALTHCARE ORGANIZATION prior to the receipt of any materials by the recipient HEALTHCARE ORGANIZATION. The recipient HEALTHCARE ORGANIZATION will identify to the donor HEALTHCARE ORGANIZATION the following:

- The quantity and exact type of requested materials,
- An estimate of how quickly the request materials are needed,
- Time period for which the materials will be needed and
- Location to which the materials should be delivered.

The donor HEALTHCARE ORGANIZATION will identify how long it will take them to fulfill the request. Since response time is a central component during a disaster response, decision and implementation should occur quickly.

b. **Documentation:** The recipient HEALTHCARE ORGANIZATION will honor the donor HEALTHCARE ORGANIZATION's standard order requisition form as documentation of the request and receipt of the materials. The recipient HEALTHCARE ORGANIZATION's security office or designee will confirm the receipt of the materials. The documentation will detail the following:
   - ○ The materials, received from the donor HEALTHCARE ORGANIZATION,
   - ○ The condition of the materials upon receipt (if applicable).
   - ○ The contact information for the party, or department that is responsible for the borrowed materials.

   The donor HEALTHCARE ORGANIZATION is responsible for tracking the borrowed inventory and documenting the original condition of the donated materials through its standard requisition forms. When returning materials, the recipient HEALTHCARE ORGANIZATION will provide the original requisition form to the donor HEALTHCARE ORGANIZATION along with the documentation of the condition of the borrowed materials being returned. The requisition form will be co-signed by the senior leadership or designee of the recipient HEALTHCARE ORGANIZATION recording the condition of the borrowed equipment.

c. **Transporting of pharmaceuticals, supplies, or equipment:** The recipient HEALTHCARE ORGANIZATION is responsible for coordinating the transportation of borrowed materials both to and from the donor HEALTHCARE ORGANIZATION. This coordination may involve government and/or private organizations, and the donor HEALTHCARE ORGANIZATION may also offer transport. Upon request, the recipient HEALTHCARE ORGANIZATION must return and pay the transportation fees for returning or replacing all borrowed materials.

d. **Supervision:** The recipient HEALTHCARE ORGANIZATION is responsible for appropriate use and maintenance of all borrowed materials.

e. **Financial and legal liability:** The recipient HEALTHCARE ORGANIZATION, to the extent permitted by federal law, is responsible for all costs arising from the use, damage, or loss of borrowed materials and for liability claims arising from the use of borrowed materials except where the donor HEALTHCARE ORGANIZATION has not provided preventive maintenance or proper repair of loaned equipment which resulted in patient injury.

f. **Demobilization procedures:** The recipient HEALTHCARE ORGANIZATION is responsible for the rehabilitation and prompt return of the borrowed materials to the donor HEALTHCARE ORGANIZATION. The recipient HEALTHCARE ORGANIZATION is also responsible for returning materials to the donor HEALTHCARE ORGANIZATION in the same condition as when they were received from the donor HEALTHCARE ORGANIZATION.

3. Jurisdiction EOC Function

The MAS provides the means for the HEALTHCARE ORGANIZATIONs to coordinate among themselves, and as a unit to integrate with Jurisdiction Public Health Department, Disaster Medical Services, police, fire, and EMS during a disaster event.

The Jurisdiction Emergency Operations Center (EOC) serves as the data center for collecting and disseminating current information about equipment, bed capacity and other HEALTHCARE ORGANIZATION resources during a disaster. The information collected by the Jurisdiction DOC/EOC is to be used only for disaster preparedness, response, and recovery.

In the event of a disaster or during a disaster drill, HEALTHCARE ORGANIZATIONs will be prepared to provide the Jurisdiction EOC with the Forms as found in the attachments to this documents. This information includes the following:

a. The total number of injury victims the HEALTHCARE ORGANIZATION is capable of receiving using the standard categories of Immediate, Delayed and Minor.

b. Total number of exam rooms currently available to accept patients

c. The number of items currently available for loan or donation to another HEALTHCARE ORGANIZATION:
- ○ Medical supplies
- ○ Pharmaceuticals
- ○ Crash carts
- ○ Defibrillators
- ○ Emergency food and water stockpile

d. The following number of personnel currently available for loan to another HEALTHCARE ORGANIZATION:
- ○ Clinicians
- ○ Physicians
- ○ Nurse Practitioner
- ○ Physician Assistants
- ○ Mental Health providers
- ○ Dentists
- ○ Other

Other Personnel
- ○ Maintenance Workers
- ○ Translators
- ○ Operations staff
- ○ Social Workers

4. Partner Buddy HEALTHCARE ORGANIZATION Concept

Each partner buddy HEALTHCARE ORGANIZATION shall standardize a set of contacts to facilitate communications during a disaster.

The procedural steps in the event of a disaster are as follows:

a. Determine the total number of patients each HEALTHCARE ORGANIZATION are able to receive.

b. The impacted HEALTHCARE ORGANIZATION contacts the partner HEALTHCARE ORGANIZATION to determine availability of equipment, supplies, and personnel. (Contacts secondary partner HEALTHCARE ORGANIZATION if primary HEALTHCARE ORGANIZATION is unable to meet needs.)

c. Impacted HEALTHCARE ORGANIZATION contacts the Jurisdiction DOC/EOC and notifies the center of its needs, how they are being met, and any unmet needs.

d. At the request of the impacted HEALTHCARE ORGANIZATION, the Jurisdiction DOC/EOC will contact other HEALTHCARE ORGANIZATIONs to alert them to the situation and to begin an inventory for any possible or actual unmet needs.

Community Health Center Mutual Aid System Memorandum of Understanding

The below signed representative agrees to the provisions of this voluntary agreement.

Signature:

_____

<Insert Health Care Organization Name here>

By _____ _____

Name, Title Date

Department _____