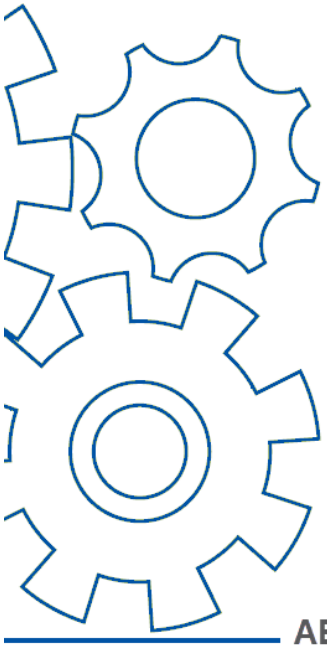
NATIONAL ASSOCIATION OF
Community Health Centers®

BUSINESS CONTINUITY PLANNING INTERACTIVE LEARNING MODULE THREE

ENSURING A HUMAN RESOURCE STRATEGY

AUGUST 2022



ABOUT THESE INTERACTIVE LEARNING MODULES

- These learning modules are the result of collaboration between the National Association of Community Health Centers (NACHC), Connecting Consulting Services, and Primary Care Development Corporation (PCDC), and Inspired Solutions Enterprises, Inc.
- They are intended to provide community health centers and primary care associations with self-guided learning tools to create and/or improve their business continuity plans and programs.
- 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

BUSINESS CONTINUITY PLANNING
INTERACTIVE LEARNING MODULE 3
ENSURING A HUMAN RESOURCE STRATEGY

Overview

Business continuity planning (BC planning) is the process of defining systems for mitigation and recovery to deal with potential threats to an organization. The Business Continuity Plan (BCP) is a framework for the continuity of pre-identified essential business functions and identified associated dependencies, recovery times and impact scores as well as to define cross-departmental components that support an organization as they begin the process of disaster recovery. A fully executed BCP will address the necessary elements health centers need to maintain their essential business functions following a disaster.

After a disaster, according to the Federal Emergency Response Administration (FEMA), of businesses without a BCP, 43% close and never reopen, 51% close within 2 years and 75% of fail within 3 years following the disaster.[1] Business Continuity Plans are intended to prepare and provide guidance to the health center during a disaster to continue providing patient care, minimizing negative financial impact and maintain operations. Comprehensive BCPs also address Disaster Recovery Planning which is focused on returning the health center to normal operations as quickly as possible following a disaster.

This course will review the rationale, scope, and components, and the recommendations and resources that are required to support the efficient development of a comprehensive BCP. This learning experience is made up of three modules:

MODULE 1: INTRODUCTION TO BUSINESS CONTINUITY PLANNING (1.5 HRS)
MODULE 2: CREATING A BUSINESS CONTINUITY PLAN (2 HRS)
MODULE 3: ENSURING A HUMAN RESOURCE STRATEGY (1 HR)

Together, these three modules provide guidance and resources for facilitating the development of a comprehensive health center BCP. Module 1 offers a comprehensive introduction that all members of the health center leadership team and board would find useful. Modules 2 and 3 provide more specific guidance for the BC planning leader and team.

Course Learning Objectives

Upon completion of these modules, learners will be able to:

1. Discuss the definition and rationale for BCPs
2. Describe the components of a comprehensive BCP
3. Draft a comprehensive BCP

Note:

1. FEMA Business Continuity Planning Suite. Business Continuity Training Part 2: Why is Business Continuity Planning Important? https://www.youtube.com/watch?v=PDW4IuQneeQ

MODULE 3: ENSURING A HUMAN RESOURCE STRATEGY

Overview of Module 3

Building on the previous BCP modules, Module 3 will focus on the critical roles of management and strategies for addressing human concerns before during and after disaster events. Wraparound services, staff management during the disaster, the incident response team, succession planning, and telecommuting are the major strategies presented.

Recommended Audience

BCP Facilitator/Manager. May also be of interest to other BC planning team members, especially the human resources and operations representative(s).

Module Objectives

Upon completion of Module 3, learners will be able to:

1. Develop an effective staff management plan and incident response team
2. Discuss the importance of employee wraparound services
3. Integrate succession planning and telecommuting strategies into your disaster response

Module 3 Chapters

1. Introduction
2. Incident Management: Key Roles
3. Incident Management: Emergency Operations Center
4. Succession Planning for Business Continuity
5. Leadership Orders of Succession & Delegations of Authority
6. Supporting Employees: Wraparound Programs
7. Supporting Employees: Communication
8. Telecommuting & Remote Work
9. Federal and State Regulations
10. Frequently Asked Questions
11. Knowledge Check

Appendix A: Glossary of Business Continuity Terms
Appendix B: Business Continuity Planning Resources Toolbox

Structure of the Chapters

Following the introduction, the major content is organized by chapter titles in the left column. Additional learning and integration activities related to the chapter are located in the right column under "Go Deeper." The number and type of activities accessed by the learner in the Go Deeper column will depend on the learner's goals and prior knowledge. Completing the Listen, Discussion, and Activity(ies) in the Go Deeper column will result in the completion of module objectives.

CHAPTER (MAIN CONTENT)	GO DEEPER (LEARN MORE, DO THE WORK)

Module 3 Time Commitment: 1 Hour Minimum

The actual amount time required to complete this self-paced, self-directed learning experience is variable. It depends upon many factors, such as learning goals, prior knowledge, how many of the Go Deeper activities and resources are utilized, and the degree to which the activities are completed as a team. Expect this module to require a minimum of 1 hour to review the main content areas and embedded audio/video files and complete the Knowledge Check.

CHAPTER 1 | INTRODUCTION

Scenario

Joanna has a primary care appointment today. She is 62 years old and is having problems with edema and pain secondary to complications of diabetes and kidney failure. She has arrived at the health center with her son and is in the waiting room. Adam is visibly upset about his mother's condition. He personally blames the U.S. healthcare "system" for not caring enough about her. Unknown to the health center staff, Adam has a criminal record and history of emotional volatility. As he arrives at check-in, he loudly states he and his mother aren't going anywhere until his mother gets what she needs to feel better - today. The registration associate and clinical staff are visibly uncomfortable with his aggressive behavior, as are other patients within earshot. While the staff members attempt to placate him, Security is called as a precaution. After Walter, one of the health center security guards, arrives and speaks with him, Adam calms down. Following the doctor's examination of Joanna, some lab tests are ordered, and she is scheduled for a follow-up visit in three days. They both leave without incident.

On the return visit a few days later, Adam arrives with his mother and seems calmer than before, even joking with the clerk at the registration desk. The staff relax. They tell Walter, whom they had called in advance as a precaution, that he can go and attend to other security assignments in the health center. The clinic waiting room is very full of patients and their family members. Joanna is called for her appointment and Adam accompanies her into the exam room. While Lisa, the medical assistant, records Joanna's vital signs, Dr. Myers knocks on the exam room door, enters, and closes the door behind him. After a few minutes, Adam can be heard yelling at Dr. Myers while Joanna can be heard trying to calm Adam down. Suddenly, the exam room door flies open, and Lisa runs out, leaving the door ajar. Adam can now be heard clearly by everyone and is shouting obscenities at Dr. Myers. Jason, the practice administrator, hurries over to the exam room to get control of the situation while Lisa calls Security. Adam becomes completely out of control, shoves Jason out of the way and walks into the waiting area, continuing to shout and gesture with his arms. He quiets for just a few seconds, then pulls a Glock 19 automatic pistol from the back of his pants and fires twice into the ceiling. Walter, who is unarmed, arrives just as the shots are fired, rushes toward Adam who turns and fires a shot in his direction. The bullet enters Walter's thigh, and he falls to the floor. Adam then forces the remaining staff and patients to barricade the doors with the clinic furniture and announces that he will shoot anyone who doesn't do what he says….

While this may not be the "typical" scenario you think of when you think, "disaster," it has the potential to end in devastating consequences in both the short and long term for the people involved and the health center operations.

THINK ABOUT: What are the potential impacts on the health center and community…

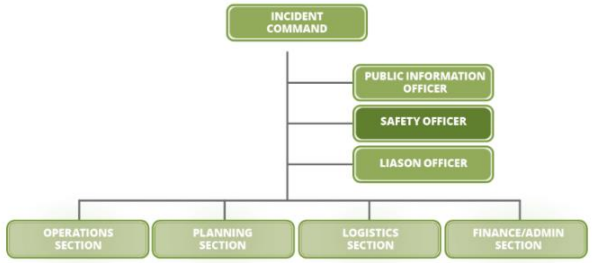
1. …if the gunman stays barricaded holding the hostages for a lengthy period of time?
2. …if patients and staff lose their lives or become permanently disabled?
3. …if the health center is found negligent or is unable to serve the community for a long period of time?
4. …if patients and staff suffer lasting effects from PTSD or survivor's guilt after the situation is resolved?
5. …if staff are unable to come back to work because of injury, fear, depression, and/or anxiety?

Having comprehensive Emergency Management and BCPs already in place will assist the health center to mobilize quickly to manage and recover from an incident such as this.

CHAPTER 2 | INCIDENT MANAGEMENT: KEY ROLES

- **Key Roles During Emergencies**
  - Key employees have major decision-making responsibility and authority for critical functions in the health center
  - During a crisis, key employees are designated to manage specific functions that will likely differ from their routine roles
  - These individuals are referred to by the title of the role they assume while managing the crisis and making business continuity and recovery decisions (e.g., the COO might become the Logistics Section Lead during a crisis, etc.)
  - In most cases, the health center CEO should focus on the overall health center response. As a key employee, board communication and taking steps toward recovery from the crisis situation are top concerns

- **Incident Command System (ICS)**
  During an emergency, health centers may implement an Incident Command System. The ICS structure can assist health centers with mounting a quick and coordinated response to crises and disruptions of business operations. Communications are integral to the ICS. This system is scalable: only roles needed should be activated. Following is the basic structure for the ICS; the structures utilized in your health center for a particular incident may require fewer or additional roles:

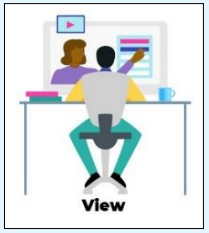


- **ICS Roles**
  - *Incident Commander (IC)* – Responsible for overall management of the ICS and has ultimate responsibility for the success of all emergency/disaster-related activities
    - Assigned at every incident, no matter how small, to someone with the necessary qualifications, experience, and authority
    - Works in collaboration with health center senior leaders to develop and execute effective action plans

GO DEEPER

ACTIVITY

We recommend that health center leaders complete **Module 1, Introduction to Business Continuity Planning** to establish a common understanding of BC Planning.



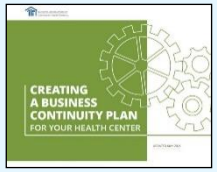
VIEW

Business Continuity Institute Webinar Series Session 3: Ensuring a Human Resources Strategy. NACHC, 2021.
Webinar (85 min)
PowerPoint Slides (PDF)

READ/REFERENCES

Incident Management. Ready.gov.

Creating a Business Continuity Plan for Your Health Center. NACHC. May 2021 (PDF)
- Incident Response (Appendix M), p. 39-40



Continuity Plan Template and Instructions for Non-Federal Entities and Community Based Organizations, FEMA, August 2018 (PDF)
- Human Resources, pp. 6-10

CHPT. 2 | INCIDENT MANAGEMENT: KEY ROLES, cont.

- **ICS Roles, cont.**
  - *Public Information Officer (PIO)* – reports to the IC and is responsible for the development and release of information about the incident; conducts media briefings, develops messaging, distributes information to incident personnel, and works closely with other members of the Incident Management Team (IMT)
  - *Safety Officer* – reports to IC and is responsible for monitoring and assessing hazardous and unsafe situations as well as developing measures for assuring personal safety; the *only* person who can supersede the IC in the event of an unsafe situation.
  - *Liaison Officer* – reports to IC and serves as the point of contact for assisting and coordinating activities between the IC and other healthcare providers and government agencies
  - *Operations Section Chief* – assists the IMT in the development of the Incident Action Plan and directs all tactical operations and resources assigned to execute the response and recovery strategy and achieve the planned goals
  - *Planning Section Chief* – supervises the collection, evaluation, processing, and dissemination of the Incident Action Plan (IAP); collects and evaluates the information that is needed for preparation of the IAP and 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* – manages logistical needs and provides facilities, services, people, and materials in support of managing the incident, such as, facilities, security, transportation, supplies, equipment maintenance and fuel, food services, and communications and information technology support
  - *Finance/Administrative Section Chief* - responsible for all financial, administrative, and cost analysis aspects of an incident, such as claims processing, contracting, and other administrative functions

The health center must have clarity among the key roles associated with the ICS and the ongoing BC Team.

GO DEEPER

LISTEN

Incident Management Structure and Roles (2:37 min). Nora O'Brien, MPA, CEM, Founder and CEO, Connect Consulting Services

ACTIVITIES

1. Identify and list your health center's current ICS key roles and designees.
2. Consider the role composition of the ongoing BC Team. Identify any areas of overlap, synergy or potential conflict with the ICS key roles. Are there any recommendations needed to assure clarity in roles and responsibilities? Share these concerns and recommendations with Executive Leadership and develop clear roles in the BCP for Incident and BC management.

CHAPTER 3 | INCIDENT MANAGEMENT: EMERGENCY OPERATIONS CENTER	GO DEEPER	
• **Emergency Operations Center (EOC)** ○ An EOC is a physical or virtual meeting place for the ICS key team members to communicate, plan and manage the emergency ○ With the full team working together, the most current information can be shared, and more timely and effective decisions made ○ A primary EOC should be established at the health center with a secondary location should the health center accommodations not be available ○ The EOC supports completion of the following incident management functions: ▪ Activation ▪ Situation Analysis ▪ Incident Briefing ▪ Action Planning ▪ Resource Management ▪ Incident Management ○ Remember that an EOC is strategic in nature, supporting on-scene activities through providing instructions and resources and communicating and coordinating services with all relevant stakeholders ***The Incident Command System and the use of an Emergency Operations Center are key ingredients for incident management and getting the health center on the path toward resuming operations as soon as possible.***		**ACTIVITY** 1. Determine if your health center has a plan for adequate space and accommodations for an EOC. Discuss the following with the BC planning team and other health center leaders: a. Are current accommodations/plans (on and off site) for the EOC conducive to managing disasters for an extended period of time? b. What logistical considerations will be needed to accommodate remote work? c. Will Key Incident Command System team members have access to the supplies and information they will need to get their jobs done? *Make a list.* Consider items like communications equipment; computers; smartphones; printers; access to the Internet and important technology applications, such as email; transportation to/from the EOC; access to news outlets; planning materials such as office supplies, whiteboards, flip charts, etc.; printed copies of emergency/disaster procedures; food & water; restroom access; etc. d. What changes will the team recommend to ensure a well-functioning EOC us accessible in the event of an extended disaster?

CHAPTER 4 | SUCCESSION PLANNING FOR BUSINESS CONTINUITY

- **What is Succession Planning**
  - Succession planning is a continuous process for preparing employees to assume different roles for everyday operations or key roles during crises
  - A successful succession plan will identify and prepare at least three individuals to serve in each key role as part of the ICS

- **Steps for Succession Planning for Business Continuity**
  1. Identify the key employees within your organization
  2. Identify the core competencies of each key position
  3. Develop job profiles and a description of the position's roles
  4. Recruit candidates
  5. Offer training, both formal (i.e., classes) and informal (coaching, mentoring, and independent study)
  6. Appoint the successor(s) to the position

- **During the Incident**
  - The incumbent assists new successor during the transition to ensure that any needed information or coaching is provided
  - Document the transition to add to the health center's incident record of major decisions and changes

- **After the Incident**
  - Evaluate effectiveness of the succession plan, transition, and outcomes
  - Identify any changes that need to be made to the succession processes

Succession Planning is an important strategy for ensuring leadership is always available and prepared to act before, during, and after a disaster.

GO DEEPER

LISTEN

Succession Planning (2:40 min). Nora O'Brien, MPA, CEM, Founder and CEO, Connect Consulting Services

READ/REFERENCE

Succession Planning: A Step-By-Step Guide. NIH, Office of HR. 2021 (PDF)

Two Types of Succession Plans and Why Your Company Needs Both. RCLCO, Real Estate Consulting. November 14, 2019. (PDF)

DISCUSS & DO

Think about what is feasible and necessary in regard to succession planning for your health center and *document in the BCP*:

1. *How many leaders should be cross trained for each ICS role?*
2. *Who are the likely candidates in current leadership roles?*
3. *Who are candidates outside of the current senior leadership circles who may be good candidates? How do we find them?*
4. *What is our training/mentoring strategy?*
5. *How will we document leadership transitions during a disaster?*
6. *What are key indicators for successful management of our succession plan and implementation?*
7. *How will we debrief after a disaster to assess our performance and outcomes?*

CHAPTER 5 | LEADERSHIP ORDERS OF SUCCESSION & DELEGATIONS OF AUTHORITY

- **Orders of Succession and Delegations of Authority During Disasters/Emergencies**
  - It's important to have plans for both Orders of Succession and Delegations of Authority *before* disaster strikes
  - While succession planning is very important for ongoing health center functions, during a disaster, knowing who is responsible for what and having leaders in place who are prepared to take on ICS key roles is even more critical for successfully navigating a disaster

- **Orders of Succession**
  - 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 current 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, and there should be at least three different persons identified as successors for the role, for example:

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

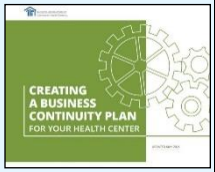
GO DEEPER

ACTIVITY

Identify the roles in your health center that are designated to serve as 1st, 2nd, and 3rd in line of leadership succession for each ICS key role and document in the BCP:

- Incident Commander
- Public Information Officer
- Safety Officer
- Liaison Officer
- Operations Section Chief
- Planning Section Chief
- Logistics Section Chief
- Finance/Administrative Section Chief

READ/REFERENCE



Creating a Business Continuity Plan for Your Health Center. NACHC. May 2021 (PDF)

- Create Leadership Orders of Success/Delegations of Authority, p. 13

Continuity Plan Template and Instructions for Non-Federal Entities and Community Based Organizations, FEMA, August 2018 (PDF)

- Succession and Delegations of Authority, pp. 10-11

CHAPTER 5 | LEADERSHIP ORDERS OF SUCCESSION & DELEGATIONS OF AUTHORITY, cont.

GO DEEPER, cont.

- **Delegations of Authority**
  - Allows certain duties of one individual/position to be assigned/ delegated to one or more persons
  - 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, e.g.:

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

- **Best Practices**
  - Be sure to always have a succession and training/mentoring plan in place for ICS key roles; work with your Human Resources/Talent Development Department to establish health center policies and procedures to support these recommendations
  - Take steps to cross-train leaders for multiple areas of responsibility and develop a coaching/mentoring support system to be used during disasters (of any size) for less experienced ICS key employees
  - You never know when disaster will strike!

Planning for Continuity of Leadership and Delegations of Authority in advance of a disaster will help ensure steady leadership and clear responsibilities for health center leaders.

CHAPTER 6 | SUPPORTING EMPLOYEES: WRAPAROUND PROGRAMS

- **Employee Assistance or "Wraparound" Programs**
  Wraparound programs are an employer-provided comprehensive and holistic method to support employees and their families when they experience trauma or loss. Consider using these strategies:
  - Whether the disaster is local or remote where employees may be traveling, assess the potential human impacts of all staff when developing your strategy
  - Encourage utilization of your health center's employee assistance plan (EAP) for direct and individualized support to manage the emotional impacts of trauma and loss and "survivor's guilt"
  - Check in with all impacted employees frequently using multiple communication channels: employees need to know what is going on and what is expected of them; avoid making false promises but use supportive and hopeful messaging
  - Be as specific as you can about next steps and instructions on what they are required to do; consider communicating work hours, procedures for reporting time off, how often they should check in and the status of the health center facilities
  - Help employees get access to recovery support provided by the health center and other organizations, such as churches, community centers, the American Red Cross, etc.

- **Wraparound Program Outcomes**
  - Individuals experiencing trauma and crises recover better when wraparound services are executed well
  - Wraparound programs participants tend to have more positive outcomes than those who do not participate
  - Outcomes include better engagement with work and team members, problem-solving, coping, job functioning, resiliency, and quality of life

Assistance and support for employees should be part of every health center's preparedness program. The supports that are essential include timely and helpful communications with employees and their families and offering a wide array of social, emotional, physical, and financial supports as appropriate.

GO DEEPER

LISTEN

What are Wraparound Services for Employees? (4:20 min). Nora O'Brien, MPA, CEM, Founder and CEO, Connect Consulting Services

READ/REFERENCE

Employee Assistance & Support. Ready.gov. 2/17/2021

Continuity Plan Template and Instructions for Non-Federal Entities and Community Based Organizations, FEMA, August 2018 (PDF)

- Additional Human Resources Considerations, pp. 12-13

DISCUSS & DO

Is our health center's EAP enough?

- Recruit the HR representative on the BC Planning team to facilitate a discussion about the health center's EAP and other wraparound supports.
- Make a list of the major features/benefits and discuss the impact these may have on supporting employees and their families during disasters that are most likely to occur in your area.
- Then, determine if additional resources or community partnerships should be secured to improve the health center's ability to support its employees during and after a disaster.
- Include these recommendations as part of the BCP.

CHAPTER 7 | SUPPORTING EMPLOYEES: COMMUNICATION

- **Good Communication is Crucial**
  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 to communicate effectively during emergencies.

- **Six Principles for Risk Communications**
  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*
  - *Principle 2: Be Right*
  - *Principle 3: Be Credible*
  - *Principle 4: Express Empathy*
  - *Principle 5: Promote Action*
  - *Principle 6: Show Respect*

- **Communication Considerations**
  - Be sure to consider diversity in the ways your employees receive communications. Ensure you are communicating with all of your employees, including those with:
    - Language differences, need for interpreters, translators, adaptive aides or sign language
    - Visual or hearing loss
    - Limited access to methods of receiving communications (e.g., no text, computer, phone, television, etc.)
  - Use a wide variety of communication tools and methods
  - 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

> "Good communication is the bridge between confusion and clarity."
> Nat Turner

GO DEEPER

LISTEN

Communication During Disasters (3:24 min). Nora O'Brien, MPA, CEM, Founder and CEO, Connect Consulting Services

READ/RESOURCES

Crisis Communications Plan, Ready.gov (2/17/2021)

Crisis & Emergency Risk Communication (CERC). CDC. January 23, 2018.

Creating a Business Continuity Plan for Your Health Center. NACHC. May 2021 (PDF)
- Risk Communications (Appendix I) p. 29

Continuity Plan Template and Instructions for Non-Federal Entities and Community Based Organizations, FEMA, August 2018 (PDF)
- Communications, pp. 14-16

ACTIVITY

1. Create a communication strategy based on the scenario presented at the beginning of this module.
   - Who is your audience?
   - What needs to be communicated and how often?
   - What methods will you use to communicate?
   - What languages?
   - What supports should be offered to patients and staff?
   - What other communication concerns should be addressed?

CHAPTER 8 | TELECOMMUTING & REMOTE WORK

During a disaster, telecommuting or remote work may be an important strategy to consider for resuming communications and health center operations as quickly as possible.

- **What is Telecommuting?**
  As a result of the COVID-19 pandemic, health centers were prompted to explore options for staff to work safely while adhering to social distancing guidelines. Telecommuting, the practice of completing work assignments away from the health center, emerged as a major go-to strategy for select employees. This is usually accomplished through technology to connect to the communication and information systems of the employer, e.g., computers, smart phones, networks, email, text messaging, virtual meetings, etc.

- **Telecommuters vs. Remote Workers**
  Employees who complete their work primarily off-site may be classified as "remote" workers instead of telecommuters. Remote implies that it is impractical for the employee to come to the workplace on a regular basis because of the distance. A "remote" worker classification may have some implications for tax and legal requirements, depending on where the employee is based.

- **Telecommuting Policy**
  - Review your health center's telecommuting policy
  - If your health center does not have a telecommuting/remote work policy, recommend that it be developed, at minimum, as part of a BCP.
  - A telecommuting policy should address:
    - Managerial oversight and communication requirements
    - Indications for temporary or long-term telecommuting
    - Reasons for revoking telecommuting permissions
    - Performance evaluation based on work output/achievement of goals
    - Risk and information security management issues unique to telecommuting

Be prepared for disaster by developing or updating your health center's telecommuting policy in advance to meet the needs of employees during disasters as well as during routine workdays.

GO DEEPER

ACTIVITY

1. Review your health center's telecommuter/remote work policy. Is it flexible enough to accommodate a short or long-term change in employee status during and after a disaster? If not, document the changes that need to be made and include your recommendations in the BCP.
2. If you need to develop a telecommuting policy, consider addressing the following elements:
   a. Objective
   b. Procedures
   c. Eligibility
   d. Equipment
   e. Security
   f. Time worked
   g. Remote Work Agreement

READ/RESOURCES

Continuity Plan Template and Instructions for Non-Federal Entities and Community Based Organizations, FEMA, August 2018 (PDF)

- Alternate Locations and Telework, pp. 17-19.

Telecommuting. TechTarget.com. Overview of telecommuting pros, cons, and the business case.

Telecommuting Policy and Procedure Sample. Society for Human Resources Management (SHRM).

LISTEN

Remote/Telecommuting Considerations (2:49 min). Nora O'Brien, MPA, CEM, Founder and CEO, Connect Consulting Services

CHAPTER 9 | FEDERAL AND STATE REGULATIONS

- **Federal vs. State Regulations – What's the Difference?**
  It's important to be familiar with both Federal and State regulations concerning what is required to obey the laws concerning how employees are managed during a disaster.
  - Federal legislation acts as umbrella laws for state-level implementation; for example, the minimum wage requirement in a particular state-enacted Shops and Establishments Acts must be in line with the Minimum Wage Act enacted at the federal level
  - State legislation addresses a number of legal concerns which can arise in the workplace, ranging from standard labor disputes to contractual questions, to discrimination and sexual harassment
  - Research your state's labors laws to determine relevant employment laws, including minimum wage laws, whistleblower protection statutes, and more

- **Federal Labor Regulations**
  - Affordable Care Act
  - Americans with Disabilities Act
  - Rehabilitation Act of 1973
  - Age Discrimination in Employment Act
  - Child Labor Laws
  - Fair Credit Reporting Act
  - Fair Labor Standards Act
  - Family and Medical Leave Act
  - National Labor Relations Act
  - Occupational Safety and Health Act
  - Retaliation and Whistleblower Laws
  - Title VII (Race, National Origin, Religion and Sex discrimination)
  - Wage and Hour Laws
  - Worker Adjustment and Retraining Notification Act

- **State Labor Regulations**
  - Child labor laws
  - Minimum wage
  - Minimum paid rest periods
  - Minimum meal periods
  - Payday requirements
  - Prevailing wages
  - Right to work
  - Worker's compensation

> "Ignorance of the law is no excuse for breaking it."
> Oliver Wendell Holmes

GO DEEPER

READ/REFERENCE

State Labor Laws, U.S. Department of Labor

Federal Labor Laws, U. S. Department of Labor

DISCUSS & DO

Ensure that the policies and procedures in your health center's BCP comply with all applicable state and federal labor regulations.

CHAPTER 10 | FREQUENTLY ASKED QUESTIONS

QUESTIONS	ANSWERS
1. ***For long term incidents, like COVID-19 or persistent wild-fire conditions, do you recommend rotating the role of the Incident Commander among several people to avoid burn-out and allow personal down time to recover?***	Absolutely. This is why, in the planning phase, you want to identify, train and mentor several people who can fill each role, including the Incident Commander. Additional people may also be identified to fill various roles after the incident/disaster begins. Generally speaking, the longer the disaster, the more individuals you will need to fill each key role. Several best practices to keep in mind are: 1. Identify and groom 3 people for each role. 2. Make an advance schedule of who is on the ICS every day of the year, in case of an incident or disaster. This will allow individuals to plan time off without disrupting the availability of key staff in the event of a disaster. 3. Identify potential ICS team roles for each senior leader position and include it in the position description. This will alert the senior leader of their potential additional responsibilities during a disaster. 4. Conduct resource/skill mapping of your employees so that you have an idea of who may be able to easily step into leadership roles during a disaster. Look past senior leadership and map skills of all employees for the best results.
2. How should decisions be made about who gets to continue working remote vs. those who have to come back to the health center after a disaster? What's fair for all employees?	The reality is that some jobs are not able to be performed remotely at all, others can be partially remote, and others fully remote. This is a question for your HR leaders and in some instances may be negotiated with HR and your immediate manager. Take stock of lessons learned and integrate them into your health center remote work policy. Your remote/telecommuting work policy may have the answers.
3. For behavioral health wraparound services, what's the best way to communicate to employees to remove any existing stigma?	It's hard to believe that there is still stigma associated with behavioral health, but it is real. General announcements and methods to get in touch with EAP or other support groups and services is a good start. Assure employees that accessing service will not trigger a notification to their team or supervisor. That said, supervisors may also suggest support that is available if the employee appears to be struggling and assure the employee that it's normal to have these concerns after a disaster event and that the supervisor and health center cares about their health, overall.
4. What will happen to telehealth services once the federal emergency funding is taken away?	Telehealth has been a resounding success for most providers of healthcare. While we can't predict the future, the hope is that there will be continued provisions for telehealth services that are permanently available.

CHAPTER 11 | KNOWLEDGE CHECK: ENSURING A HUMAN RESOURCES STRATEGY

Check your understanding of some of the major concepts shared in this module. Review sections of the module for which you are unsure of the answers.

QUESTIONS

1. During emergencies, key employees are referred to by their job titles at the health center. True/False
2. The following are true about Incident Command Systems (ICS) (select all that apply):
    a. Scalable
    b. Facilitate Communications
    c. Are activated in times of emergencies
    d. Members have distinct roles
    e. All of the above
3. Where possible, a primary Emergency Operations Center (EOC) should be established _____, with a secondary location _____ (fill in the blanks)
    a. Offsite
    b. Onsite
    c. Offsite or virtual
    d. Onsite or virtual
    e. Nearest available facility
4. The steps involved in succession planning are (put the following steps in order from first to last):
    a. Offer formal and informal training
    b. Recruit candidates
    c. Identify the key employees within your organization
    d. Develop job profiles and a description of the position's roles
    e. Identify the core competencies of each key position
    f. Appoint successors
5. Continuity of leadership during an emergency is critical to ensure continuity of essential functions. True/False
6. Wraparound programs are designed to ensure (select the best response):
    a. Employees are able to get to their job during an emergency
    b. Patients have alternative health care options
    c. Employees have holistic care and support during a crisis
    d. People stay warm during a snow emergency
    e. All of the above
7. The following are principles for communicating during an emergency (select all that apply):
    a. Be Graphic
    b. Be First
    c. Be Right
    d. Be Complacent
    e. Be Credible
    f. Be Indifferent
8. When communicating during disasters, choose one reliable method of communication and stick with it. True/False
9. Telecommuting and remote work are effective strategies to employ during an emergency or disaster. True/False
10. State labor laws may vary greatly from state to state. True/False

KNOWLEDGE CHECK ANSWERS		
1. FALSE 2. E 3. B, C 4. C, E, D, B, A, F	5. TRUE 6. C 7. B, C, E	8. FALSE 9. TRUE 10. TRUE

Congratulations!

You have completed the final module of the NACHC BCP Learning Series.

APPENDIX A | GLOSSARY OF BUSINESS CONTINUITY PLANNING

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.

Business Continuity: The capability to continue essential business processes under all circumstances.

Business Continuity Planning (BC Planning): An all-encompassing, "umbrella" term used to describe the comprehensive process of planning for the recovery of operations in the event of a disruptive/disaster event.

Business Continuity Plan (BCP): The business continuity plan is a document that defines recovery responsibilities and resources necessary to respond to a disruption to business operations.

Business Impact Analysis (BIA): A review of current operations, with a focus on business and clinical essential services, to determine the effect that a business disruption would have on normal business operations. Impacts are measured in either quantitative or qualitative terms. This information is used to drive the recovery planning process, the potential recovery solutions, and the amount of expenditure required to support the backup of certain business operations. The BIA identifies critical agency functions and supporting technology and support functions necessary to meet the Recovery Time Objective (RTO) and Recovery Point Objective (RPO).

Crisis Communication Plan: a plan developed to share information quickly and accurately with important stakeholders following a disaster or emergency.

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.

Critical Process Essential functions that are important to the mission of the organization and must be maintained during an emergency event.

Cyber Crime: A criminal act involving computers or computer networks. Cybercrimes 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 Security Analysis: the process of analyzing potential threats to the security of an organization's computers, servers, mobile devices, electronic systems, networks, and data from attacks. The term applies in a variety of contexts, from business to mobile computing, and can be divided into a few common security categories: *Network, Application, Information and Operational*.

Disaster: A sudden, calamitous event that seriously disrupts the functioning of a community or society and causes human, material, and economic losses that exceed the community's or society's ability to cope using its own resources.

Disaster (healthcare perspective): Any situation where the incident, numbers of patients, or severity of illness impacts or exceeds the ability of the facility or system to care for them.

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.

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 Continuity Plan is an ongoing process supported by senior management and is funded by the organization. It is usually the introduction to the plan.

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.

Hazard: A hazard is related to the probability that a natural event, or one caused by human activity, may occur in the facility or region; 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.

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.

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.

Jurisdiction DOC/EOC (Jurisdiction Department Operations Center/Emergency 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.

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.

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.

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.

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.

MAS: Mutual Aid System

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).

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.

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.

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.

Process: A systematic series of activities or tasks that produce a specific end.

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.

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.

Recipient healthcare organization: The impacted facility. The healthcare organization where disaster patients are being treated and have requested personnel or materials from another facility.

Recovery Point Objective (RPO): The point in time to which data must be restored in order to resume processing transactions. RPO is the basis on which a data projection strategy is developed.

Recovery Time Objective (RTO): The time it takes to restore data and system/application functionality that must be restored in order to resume processing transactions.

Risk: A risk is related to the probability, based on history, that certain identified hazards will occur. These circumstances are closely related not only history and to the level of exposure and impact of an event, but to the vulnerability to the effects of the event. The effect of hazard combined with vulnerability.

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.

Staff (or personnel): Staff or personnel are employees of a specific healthcare organization.

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

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

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

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.

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

For a more extensive glossary check: FEMA's Glossary of Terms

APPENDIX B | BUSINESS CONTINUITY PLANNING RESOURCES TOOLBOX

Hint: Use key word search to find resources (CTRL + F)

1. Business Case for Remote Work – For Employers, Employees, the Environment, and Society Design Public Group and Global Workplace Analytics. 2021. https://globalworkplaceanalytics.com/download/235613/
2. Business Continuity Business Case Template. Castellan. Note: Email address and job title are required to download this resource. https://castellanbc.com/template/business-continuity-business-case/#form
3. Business Continuity Plan Example A. NACHC.
4. Business Continuity Plan Example B. NACHC.
5. Business Continuity Planning Institute Webinar Series. NACHC. 2021.
   a. Introduction to Business Continuity Planning webinar PowerPoint presentation, NACHC, 2021. https://protect-us.mimecast.com/s/mK89COY2DyIkwkmtrsasZ Webinar: https://www.youtube.com/watch?v=NVhrCTCMLm4
   b. Creating a Business Continuity Plan webinar PowerPoint presentation, NACHC, 2021. https://protect-us.mimecast.com/s/orGJCQW2G0sL9LjuAYV7D Webinar: https://www.youtube.com/watch?v=zduGYCeQTnE
   c. Ensuring a Human Resource Strategy Webinar PowerPoint presentation, NACHC, 2021. https://protect-us.mimecast.com/s/TWSpCVOkjPu8X8oTEVuh4 Webinar: https://www.youtube.com/watch?v=yO3BABszjJc
6. Business Continuity Planning Interactive Learning Series. NACHC. 2022.
   a. Introduction to Business Continuity Planning
   b. Creating a Business Continuity Plan
   c. Ensuring a Human Resource Strategy
7. Business Continuity Planning Suite. FEMA. https://www.ready.gov/business-continuity-planning-suite
8. Business Continuity Planning Suite. Business Continuity Training Part 2: Why is Business Continuity Planning Important? FEMA. https://www.youtube.com/watch?v=PDW4IuQneeQ
9. Business Impact Analysis. 2021. Ready.gov: https://www.ready.gov/business-impact-analysis
10. Business Continuity Training Introduction (video). Ready.gov. https://www.youtube.com/watch?v=R1oIQ4Y_EHY&list=PL720Kw_OojIly2uSz0VTHM-Whk-Su8Ucy&index=1
11. CMS Emergency Preparedness Final Rule Updates - Rural Health Clinic / Federally Qualified Health Center Requirements, Effective March 26, 2021. https://files.asprtracie.hhs.gov/documents/aspr-tracie-cms-ep-rule-rhc-fqhc-requirements.pdf
12. Common Disasters Across the U.S. American Red Cross. https://www.redcross.org/get-help/how-to-prepare-for-emergencies/common-natural-disasters-across-us.html#all
13. Continuity Plan Template and Instructions for Non-Federal Entities and Community Based Organizations. FEMA, August 2018. https://www.fema.gov/sites/default/files/2020-10/non-federal-continuity-plan-template_083118.pdf
14. COVID-19 Response Resources. NACHC. https://www.nachc.org/clinical-matters/current-projects/building-capacity-of-community-health-centers-to-respond-to-covid-19/
15. Creating a Business Continuity Plan For Your Health Center, May 2021. NACHC. https://www.nachc.org/wp-content/uploads/2020/11/Business-Continuity-Manual_Interactive-1.pdf
16. Crisis & Emergency Risk Communication (CERC). CDC. January 23, 2018. https://emergency.cdc.gov/cerc/
17. Cybersecurity. Ready.gov. 11/18/2020. https://www.ready.gov/cybersecurity
18. Cybersecurity in Healthcare. Healthcare Information and Management Systems Society (HIMSS). The Healthcare Information and Management Systems Society (HIMSS) discusses the three goals of cybersecurity: protecting the confidentiality, integrity and availability of information, also known as the "CIA triad." https://www.himss.org/resources/cybersecurity-healthcare
19. Disaster Declarations for States and Counties. FEMA. Explore historic federal disaster declarations by state, county, hazard, and year. https://www.fema.gov/data-visualization/disaster-declarations-states-and-counties
20. Employee Assistance & Support. Ready.gov. 2/17/2021
21. Engaging in Succession Planning. Society for Human Resource Management (SHRM). 2017. Detailed overview of succession planning, rationale, methods, and business case. May be most appropriate for HR professionals. https://www.shrm.org/resourcesandtools/tools-and-samples/toolkits/pages/engaginginsuccessionplanning.aspx
22. Federal Labor Laws. U. S. Department of Labor. https://www.dol.gov/general/aboutdol/majorlaws
23. Glossary of Terms. FEMA. https://www.fema.gov/pdf/plan/glo.pdf
24. Good Samaritan Hospital: Business Continuity Guide for Critical Business Areas (PDF, Sample/Template). https://www.calhospitalprepare.org/sites/main/files/file-attachments/goodsam.pdf
25. Guide to Developing an Effective Business Continuity Plan. 2020. Noggin. https://www.noggin.io/hubfs/Noggin%20-%20Guide%20to%20Effective%20BCP%20-%20December%202020.pdf
26. Hazard Information Sheets Suite. FEMA. https://www.ready.gov/sites/default/files/2021-01/ready_full-suite_hazard-info-sheets.pdf

27. Healthcare Business Continuity Management and Disaster Recovery— No Longer an Afterthought in Today's World. 2019. Association of Healthcare Internal Auditors (AHIA) and Crowe. https://ahia.org/getattachment/news/White-Papers/AHIA-Crowe-Whitepaper.pdf/?lang=en-US
28. HIT Solution for Clinical Care and Disaster Planning: How One Health Center in Joplin, MO Survived a Tornado and Avoided a Health Information Disaster. (Shin P, Jacobs F.) Online J Public Health Inform. 2012;4(1):ojphi.v4i1.3818. doi: 10.5210/ojphi.v4i1.3818. Epub 2012 May 17. PMID: 23569622; PMCID: PMC3615799. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3615799/
29. Hospital Continuity Planning Toolkit. 2012. California Hospital Association Hospital Preparedness Program Hospital Continuity Planning Workgroup. https://www.calhospitalprepare.org/sites/main/files/file-attachments/hcp_toolkit_1.pdf
30. Hospital Incident Command System, Internal Scenarios. 2006. Emergency Management Services Authority of California. https://emsa.ca.gov/hospital-incident-command-system-internal-scenarios/
31. Hospital Incident Command System, External Scenarios. 2006. Emergency Management Services Authority of California. https://emsa.ca.gov/hospital-incident-command-system-external-scenarios/
32. How to Make a Business Case. Workfront.com. Template for making a business case. https://www.workfront.com/project-management/life-cycle/initiation/business-case
33. Incident Management. Ready.gov. 5/26/2021. https://www.ready.gov/incident-management
34. Interactive Disaster Map. The Ready Store. Learn the likelihood of specific natural disasters affecting your state. https://www.thereadystore.com/natural-disaster-map/
35. Joint Commission Emergency Management Requirements. https://store.jcrinc.com/assets/1/7/cc_hap_em.pdf
36. PrepTalks. FEMA. 33 presentations by subject-matter experts and thought leaders to spread new ideas, spark conversation, and promote innovative leadership for the issues confronting emergency managers now and over the next 20 years. https://www.youtube.com/playlist?list=PL720Kw_OojIJiYKDZQwKG7HAgV_qNjbLB
37. ReadyBusiness Toolkit. FEMA. The Ready Business Toolkit series includes hazard-specific versions for earthquake, hurricane, inland flooding, power outage, and severe wind/tornado. Toolkits offer business leaders a step-by-step guide to build preparedness within an organization. Each toolkit contains the following sections: Identify Your Risk; Develop A Plan; Take Action; Be Recognized and Inspire Others. https://www.ready.gov/business
38. Rural Health Clinic / Federally Qualified Health Center Requirements CMS Emergency Preparedness Final Rule Updates Effective March 26, 2021. https://files.asprtracie.hhs.gov/documents/aspr-tracie-cms-ep-rule-rhc-fqhc-requirements.pdf
39. State Labor Laws, U. S. Department of Labor. https://www.dol.gov/agencies/whd/state
40. State of Remote Work 2021. Owl Labs and Global Workplace Analytics. https://globalworkplaceanalytics.com/download/239489/
41. Succession Planning: A Step-By-Step Guide. NIH, Office of HR. 2021. https://hr.nih.gov/sites/default/files/public/documents/2021-03/Succession_Planning_Step_by_Step_Guide.pdf
42. Telecommuting. TechTarget.com. Overview of telecommuting pros, cons, and the business case. https://www.techtarget.com/searchmobilecomputing/definition/telecommuting
43. Telecommuting Policy and Procedure Sample. Society for Human Resources Management (SHRM). https://www.shrm.org/resourcesandtools/tools-and-samples/policies/pages/telecommuting_policy.aspx
44. Two Types of Succession Plans and Why Your Company Needs Both. RCLCO, Real Estate Consulting. November 14, 2019. https://www.rclco.com/wp-content/uploads/2019/11/The-Two-Types-of-Succession-Plans-and-Why-Your-Company-Needs-Both.pdf
45. Types of Disasters. SAMHSA. https://www.samhsa.gov/find-help/disaster-distress-helpline/disaster-types
46. Wakefield- Brunswick. Santa Cruz County Business Continuity Plan Example (template). https://www.santacruzhealth.org/Portals/7/Pdfs/HPP/CO_LTC_SNF_Template.docx
47. What is Succession Planning? 7 Steps to Success. Robert Half. 10/3/2021. Here are seven tips for kick-starting the succession planning process at your company. https://www.roberthalf.com/blog/management-tips/7-steps-to-building-a-succession-plan-for-success
48. What's a Business Continuity Plan? FEMA. Ready.gov video available on YouTube. https://www.youtube.com/watch?v=R1oIQ4Y_EHY&list=PL720Kw_OojIIy2uSz0VTHM-Whk-Su8Ucy&index=1
49. Yale Guide to Business Continuity and Recovery Planning – General. 2016. Yale Office of Emergency Management. https://emergency.yale.edu/sites/default/files/files/Guide-BCP-General-Audience.pdf