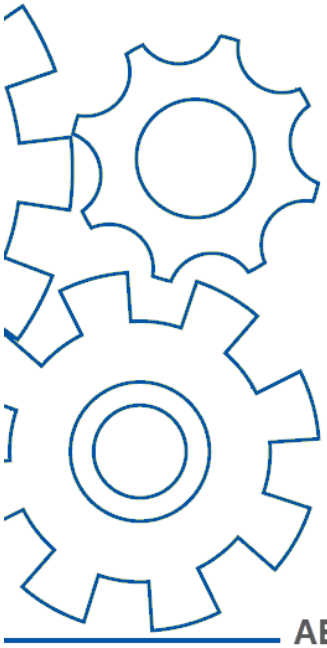
NATIONAL ASSOCIATION OF
Community Health Centers®

BUSINESS CONTINUITY PLANNING INTERACTIVE LEARNING MODULE TWO

CREATING A BUSINESS CONTINUITY PLAN

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 2
CREATING A BUSINESS CONTINUITY PLAN

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 2: CREATING A BUSINESS CONTINUITY PLAN

Overview of Module 2

Module 2 describes the key components, rationale, processes, and recommended resources to complete the development of a comprehensive BCP.

Recommended Audience

BCP Facilitator/Manager. May also be of interest to leaders working closely with the BCP Facilitator to develop the plan.

Module Objectives

Upon completion of Module 2, learners will be able to:

1. Detail the key elements of a business continuity plan
2. Discuss the process of using the business continuity tool
3. Provide information needed to develop a successful cybersecurity plan

Module 2 Outline

1. Introduction
2. Preparing the Health Center for Business Continuity Planning
3. Business Continuity Team
4. Business Continuity Plan Core Components
5. Hazard Vulnerability Analysis
6. Cybersecurity in Healthcare and Impact Analysis
7. Business Impact Analysis
8. Mitigation Strategy
9. Recovery Strategies
10. Business Continuity Plan Implementation and Sustainability
11. Executive Summary & Putting It All Together
12. Frequently Asked Questions
13. Knowledge Check
14. Preparation for Module 3: Ensuring a Human Resources Strategy

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 2 Time Commitment: 2 Hours Minimum

The actual amount time required to complete this self-paced, self-directed learning experience is variable depending 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 2 hours to review the main content areas and embedded audio/video files and complete the Knowledge Check.

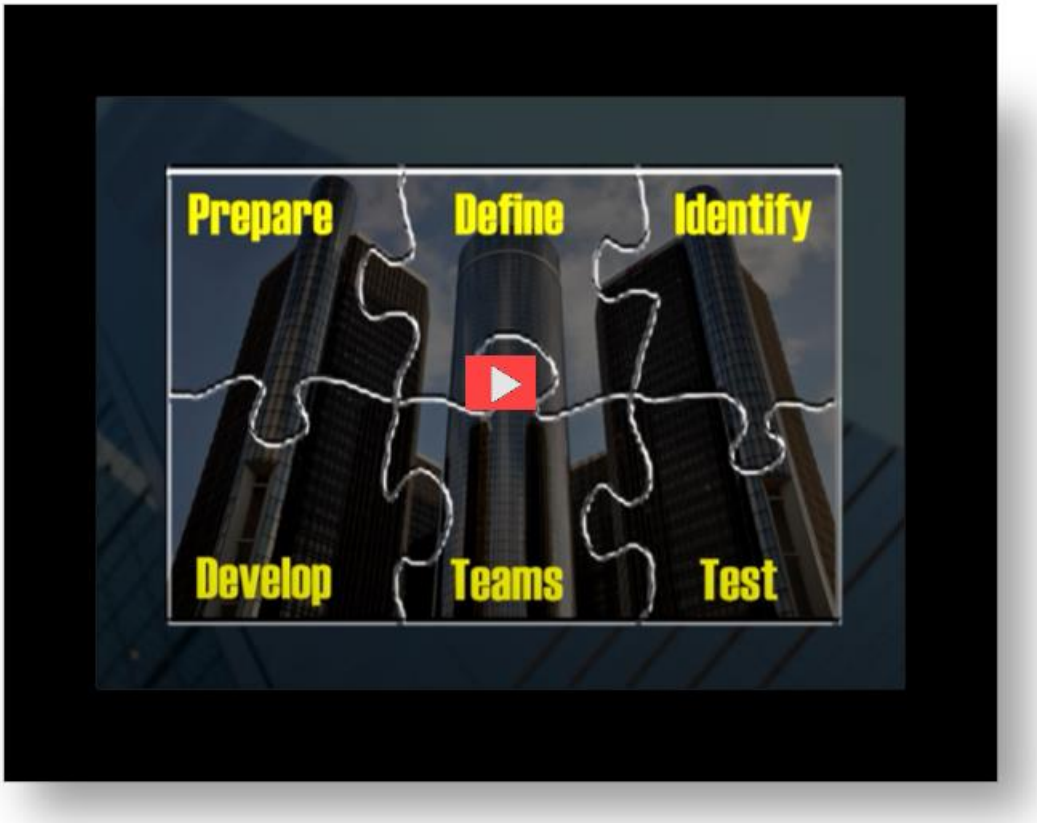
CHAPTER 1 | INTRODUCTION

The ultimate goal of a Business Continuity Plan (BCP) is to enable critical business functions to continue uninterrupted during an emergency or disaster. The BCP is intended to be a dynamic plan that 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 to provide care for the community and reduce the economic impact to the facility during a disaster as well as allows it to maintain its critical business and logistical functions.

A comprehensive and well thought-out BCP goes beyond emergency management and provides guidance for the health center to fully recover normal business operations in a timely manner.

> *"Though they may intersect with emergency management plans, which are concerned with keeping patients and staff safe from harm during a disaster, business continuity plans (BCPs) are focused on continuing operations when main systems are down." (16, p.3).*

What's best way to get started developing a BCP? This FEMA video offers some general guidance and will help get you ready for this module.



This video, produced by FEMA as part of its Business Continuity Planning Suite and give some insight into how to get started developing your plan. View the full video on YouTube: Ready.gov - Business Continuity Training Part 3: What's the Business Continuity Planning Process? (1.35 min)
https://www.youtube.com/watch?v=e1oWmHn-sNM&list=PL720Kw_OojIly2uSz0VTHM-Whk-Su8Ucy&index=6

CHAPTER 2 | PREPARING THE HEALTH CENTER FOR BC PLANNING

"A winning effort begins with preparation."
Joe Gibbs

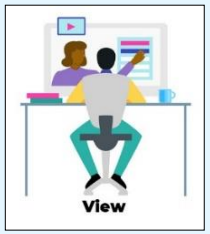
- **Preparing Health Center Leaders**
  Before beginning the work of developing a BCP, the health center senior leadership must be prepared for engaging in and supporting the process. Executive and board **support** of the BCP is critical to developing, implementing, and sustaining a viable plan. Health center leadership should understand the benefits of developing the BCP and the risks associated with not having one. It's a good idea to ensure that all health center leadership complete ***Module 1: Introduction to Business Continuity Planning*** to prepare them for their roles and commitments in the design and implementation of the plan.

- **The Role of Senior Leadership in the BC Planning Process**
  The organization's senior management team is responsible for overseeing the business continuity planning process, which 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 as well as after each exercise and real-life event
  - Ensuring employees are trained and aware of their roles in the implementation of the BCP, including all staff that serve in delegated positions (we will discuss delegation of authority a bit later)
  - Reviewing the BCP testing program and test results on a regular basis. This is accomplished by annual or semi-annual exercises
    - Note that these exercises can also meet the CMS requirement for Emergency Management Plan exercises

GO DEEPER

ACTIVITY

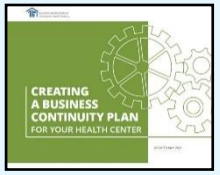
We recommend that health center leaders complete **Module 1, Introduction to Business Continuity Planning** to establish a common understanding of BC Planning.



VIEW

Business Continuity Institute Webinar Series Session 2: Creating a Business Continuity Plan. NACHC, 2021.
Webinar (92 min)
PowerPoint Slides (PDF)

READ/RESOURCES



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

Healthcare Business Continuity Management and Disaster Recovery— No Longer an Afterthought in Today's World. Association of Healthcare Internal Auditors (AHIA) and Crowe. (PDF)

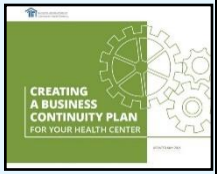
CHAPTER 2 | PREPARING THE HEALTH CENTER FOR BC PLANNING, cont.	GO DEEPER	
• **Board of Directors Roles and Responsibilities** The essential roles of the Board of Directors are to ensure that the health center is prepared to handle any disruption and remain prepared to fulfill its mission in the event of a disaster. The Board's ongoing roles and responsibilities for BC are to ○ Ensure policies and procedures are in place and effective in managing disasters ○ Review and acknowledge routine and emergency revisions to the plan. ○ Provide consistent support for training, assessment, and monitoring, and maintenance of emergency preparedness and business continuity plans • **Preparing the Health Center** As the planning process gets underway, don't forget to begin to prepare the health center staff for what's to come. Some ideas to consider before, during and after the development of the BCP include: ○ Develop talking points about BCPs for health center leaders to share with their teams; review the talking points in C-suite level and board meetings ○ Include reminders about aspects of the BCP that impact the entire health center in general internal business communications, such as the newsletter or intranet ○ Include aspects of the health center BCP as a regular agenda topic in executive and department level meetings on a rotating schedule throughout the year; focus these discussions on critical aspects of the BCP that may require significant time and or resources, for example: ▪ upgrading IT/data management systems ▪ making significant changes to health center operations or infrastructure ○ Remind department leaders to share information impacting the BCP with the BCP Manager. ***Preparing the health center to actively participate in the BC Planning process is critical to successful development and a smooth implementation.***		**LISTEN** Overview of BCP Planning Team Composition and Rationale (2 min). Amanda Cooper, MPH, Planning Specialist, Connect Consulting Services.

<table>
<tr><th>CHAPTER 3 | BUSINESS CONTINUITY PLANNING TEAM</th><th colspan="2">GO DEEPER</th></tr>
<tr><td rowspan="2">

- **BC Planning Team Leadership**
  A BCP Manager should be appointed to lead development and oversee implementation of the plan. Ideally, they should be part of the senior management team. Oftentimes, this role is taken on by the Operations functions of the health center, however, the BCP manager may be appointed based on other factors, such as leadership qualities, project management acumen, experience with disaster management, etc. The BCP Manager's overall responsibilities include leading the BC Planning Team and/or health center staff to:
  - Develop and maintain the health center's BCP and procedures; reviews, revises, and expands existing plans and protocols
  - Conduct risk assessments for various departments and functions, analyze potential business impact of unpredictable business interruptions such as natural disasters, security breach, legal claims, and market disruptions
  - Create and facilitate practice drills for plan execution
  - Develop and provide staff training on the BCP policies and protocols
  - Work with health, safety, and security staff and local, state, and federal agencies to align the health center's emergency management plan and BCP with established best practices and community standards
  - Maintain current knowledge of best practices in BC Planning for health centers

- **The Business Continuity Team is Multidisciplinary by Design**
  A robust BCP requires information on all aspects of the health center's operations. 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 multi-disciplinary team. When building the BC Planning Team, it is important that they are able to work with and gather information from all the departments within the health center.

</td><td> 
</td><td>**ACTIVITY**
After considering the organization and structure of your health center, make a list of departments needing representation on the BC Planning Team as ongoing and ad hoc participants.</td></tr>
<tr><td> 
</td><td>**DISCUSS/DO**
If the BCP Manager has not yet been identified, C-suite leaders should discuss and recommend likely candidates for the role based on:
○ Their history of exemplifying the health center's vision and values in their work
○ Experience with or understanding of BCP/Emergency Management
○ Familiarity with the operations of most departments in the health center
○ Project management skills
○ People management Skills
○ Enthusiasm for the work</td></tr>
</table>

CHAPTER 3 | BUSINESS CONTINUITY PLANNING TEAM, cont.	GO DEEPER	
• **BC Planning Team Department Representation** The BC Planning Team leads the research and builds the BCP while collaborating with health center departments to ensure accuracy of the completed plan. This team may also be appointed to oversee training, testing, reviewing, and updating the plan and meet on a regular basis for these purposes (e.g., quarterly). Leaders from all major departments in the health center (with at least one C-suite leader) should be represented on the BC Planning Team, but at minimum should include: ○ Medical ○ Clinical ○ Administrative Functions ○ Information Technology/Cyber Security ○ Facility Operations ○ Finance and Accounting ○ Human Resources ○ Risk Management & Safety ○ Legal ○ Communications/Public Information Additional departments may be identified for inclusion based on the mission and scope of services at the health center. An important function of the BC Planning Team is to work with health center departments to understand the critical processes required for them to operate effectively. Disruptions to staffing, supply chain, accessibility to the facility, utility/equipment failures, data inaccessibility, etc., may impact different departments to varying degrees. Note that all departments may not be needed for continuous participation and may be called upon only when their area of expertise or plan review and feedback is needed. Each of these members brings technical and advanced knowledge of their field that is central to the development of a sound BCP. ***The BC Planning Team represents the major functions/ departments required to operate the health center and includes a BCP Manager who leads the project and implementation.***		**LISTEN** Key BC Planning Team Departments (6 min). Amanda Cooper, MPH, Planning Specialist, Connect Consulting Services.
		**READ/RESOURCES** Creating a Business Continuity Plan for Your Health Center. NACHC. May 2021 (PDF). ○ Multidisciplinary Team Checklist, p. 18 ○ Health Care Processes Sample List, p. 19 

CHAPTER 4 | BCP PLAN CORE COMPONENTS

- **The Core Components of the BCP**
  While these may differ slightly among healthcare centers, BCPs consist of these core elements:
  - Hazard Vulnerability Analysis (HVA)
  - Cybersecurity Impact Analysis (CIA)
  - Business Impact Analysis (BIA)
  - Mitigation Plan/Strategy
  - Leadership Orders of Succession/Delegations of Authority
  - Recovery Strategies
  - Communication Plan (internal and external)
  - BCP Implementation and Maintenance Procedures (including implementation timeline, education, training, and exercises)
  - Executive Summary (this is the introduction to the final BCP document, but is the last component written)

  Each of these components will be reviewed in the following sections.

BCPs may differ among health centers but most contain these core elements.

GO DEEPER

READ/RESOURCES
Business Continuity Planning Toolkits

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

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

Business Continuity Planning Suite. Ready.gov. Includes interactive tools to create both Business Continuity and Disaster Recover Plans and Tools for running table-top disaster drills for planning, education, and practice.

Hospital Continuity Planning Toolkit. California Hospital Association Hospital Preparedness Program Hospital Continuity Planning Workgroup. (PDF)

Guide to Developing an Effective Business Continuity Plan. 2020. Noggin (PDF)

Healthcare Business Continuity Management and Disaster Recovery— No Longer an Afterthought in Today's World. Association of Healthcare Internal Auditors (AHIA) and Crowe. (PDF)

CHAPTER 5 | HAZARD VULNERABILITY ANALYSIS (HVA)

- **What is a Hazard Vulnerability Analysis?**
  The hazard vulnerability analysis (HVA) is a CMS requirement and is the process used to identify the health center's risk for disruption of operations by specific disasters. It answers the questions:
  - What hazards are most likely to involve your health center?
  - And what should be done now to mitigate potential negative impacts?

- **Who completes the HVA?**
  The BC Planning Team coordinates the completion of the HVAs in collaboration with health center leaders and committees (i.e., Environment of Care, Emergency Management, etc.), Be aware that there are many free tools available online to complete an HVA. One of the most popular is the Kaiser Permanente HVA (see activity).

- **The HVA May Include:**
  - Identifying risks (based on probability, history, and impact)
  - Identifying any control weaknesses and/or single points of failure
  - Pinpointing, selecting, and documenting mitigation/corrective measures (including costs) to mitigate the identified risks (these carry over to the comprehensive Mitigation Strategy)
  - Identifying the top 3-5 vulnerabilities for which mitigation plans should be developed
  - 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 provide the leadership team with a formal written summary.

The HVA should be revisited annually to ensure the health center maintains preparedness due to changes in the climate, advances in technology, etc.

There are many tools readily available to conduct HVAs, so there's no need to "reinvent the wheel." Several tools are shared as resources in this learning module.

GO DEEPER

LISTEN

Hazard Vulnerability Analysis Considerations (8:42 min). Amanda Cooper, MPH, Planning Specialist and Nora O'Brien, MPA, CEM, Founder and CEO, Connect Consulting Services

ACTIVITIES

1. Utilize at least one of the following tools (also referenced in "Module 1, Introduction to BC Planning") to identify the likelihood of certain disasters impacting your health center's operations:
   - Common Disasters Across the U.S. American Red Cross.
     Learn what disasters are most common in your region.
   - Interactive Disaster Map. The Ready Store.
     Learn the likelihood of specific natural disasters affecting your state.
   - Disaster Declarations for States and Counties. FEMA.
     Explore historic federal disaster declarations by state, county, hazard, and year.

CHAPTER 5 | HAZARD VULNERABILITY ANALYSIS (HVA), cont.	GO DEEPER	
		**ACTIVITIES, cont.** 2. Complete a Hazard Vulnerability Analysis for your health center. Resources: ○ NACHC Hazard Vulnerability Analysis Template, Appendix E (p. 20) Creating a Business Continuity Plan for Your Health Center. NACHC. May 2021 (PDF).  ○ Kaiser Permanente Hazard Vulnerability Analysis. This interactive tool is an Excel spreadsheet that calculates your risk for being impacted by specific disasters. Instructions included. ○ Or HVA of your choice 3. After completing the HVA, document the results to include in your BCP. Discuss the following with the BC Planning Team and other contributors: 1. *What are the top 3-5 vulnerabilities for which a mitigation plan should be developed?* 2. *How many of these vulnerabilities already have supporting documentation or policies in effect to address them?* 3. *Which vulnerabilities do you believe will require the development of new policies/procedures or additional resources/dollars to remedy or mitigate, and who should be included in the development?* 4. Prepare this discussion to include in the BCP HVA section.

CHAPTER 6 | CYBERSECURITY IMPACT ANALYSIS AND PLANNING

- **What is Cybersecurity?**
  Cyber security is the practice of defending 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.*

- **Why is attention to Cybersecurity important for the BCP?**
  - The cybersecurity risk assessment is considered alongside the Business Impact Analysis (BIA) because a cybersecurity incident is likely to cause harm to a health centers operations, 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 of the facility
  - Healthcare facilities are very appealing to cybercriminals because they collect financial, medical, and other personal data of its patients and employees, and vendors; compromise can occur through various means, such as unauthorized access to information, hacking, phishing, and loss or theft of laptops or smartphones, among others
  - All businesses that use networks can be targeted for cyberattacks and the number of data breaches in healthcare continues to grow annually

> "Cybersecurity is much more than an IT topic."
> Stephane Nappo

GO DEEPER

LISTEN
Overview of Cybersecurity (2 min). Amanda Cooper, MPH, Planning Specialist, Connect Consulting Services.

READ/RESOURCES
Case Example: An HIT Solution for Clinical Care and Disaster Planning: How One Health Center in Joplin, MO Survived a Tornado and Avoided a Health Information Disaster Online Journal of Public Health Informatics

DISCUSS/DO
Using the document, An HIT Solution for Clinical Care and Disaster Planning: How One Health Center in Joplin, MO Survived a Tornado and Avoided a Health Information Disaster, discuss:

1. *What are the potential similarities and differences in how your health center would manage a similar situation?*
2. *How prepared for disaster is the IT vendor for your health center?*
3. Identify a few strategies shared in the article that your health center may find useful in a similar situation.

CHAPTER 6 | CYBERSECURITY IMPACT ANALYSIS AND PLANNING, cont.

- **What are the health center's major considerations for Cybersecurity?**
  - Your health center's Chief Information Security Officer and/or Chief Information Officer's involvement in conducting the analysis and plan are critical for successful integration into the BCP
  - Patients need to understand and have access to secure methods for communicating personal, confidential, and financial information with their health care center and providers, including patient portals, telehealth, secure messaging, etc.
  - Health Center Staff must understand health center cybersecurity policies and expectations, including strong security measures for log in/out, email management, data sharing, use of encrypted vs. public networks, recognition of and actions to take when confronted with a potential threat or loss of equipment, etc.; ongoing training/testing of staff should be conducted to ensure an understanding of and adherence to, policy
  - Keep staff informed about current threats that are critical for maintaining cybersecurity
  - Vendors/Suppliers doing business with the health center should be able to demonstrate a high level of cybersecurity awareness with policies and procedures in place to prevent or mitigate an attack; cybercriminals are known to attack supply chains to find access to their customers' IT systems

- **Cybersecurity Impact Analysis and Plan Components**

  A cybersecurity impact analysis and plan contains the following 6 steps:
  1. Define Information Value
  2. Identify Critical Systems Assets
  3. Identify Threats to Cybersecurity
  4. Identify Vulnerabilities
  5. Develop a Set of Controls
  6. Develop Cybersecurity Action Plan

Conducting the cybersecurity analysis and plan should rely heavily upon the expertise of the health center Chief Information Security Officer/Chief Information Officer and/or external consultants.

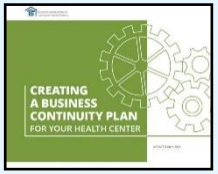
GO DEEPER

LISTEN

Cybersecurity Impact Analysis and Plan Components (4:20 min). Amanda Cooper, MPH, Planning Specialist, Connect Consulting Services.

READ/RESOURCES

Creating a Business Continuity Plan for Your Health Center. NACHC. May 2021 (PDF)
- NACHC Cybersecurity Impact Analysis Template, Appendix F (pp. 21-23)



ACTIVITIES

1. Meet with your health center cybersecurity expert (CSIO, CIO or other) to determine how they will work with the BC Planning Team to conduct the cybersecurity analysis and mitigation plan for the health center, and which tools or question set will be used.
   - Review the *Cybersecurity Impact Analysis Template* checklist referenced above to generate discussion about the cybersecurity status of the health center.
2. Determine which roles each team member will take. If external resources are needed consult with your board of directors and health center IT leaders to identify an appropriate consultant or company.
3. Document the plan for conducting the cybersecuirty analysis and mitigation plan. Note that the results of this process overlap with the BIA and Mitigation Plan.

CHAPTER 7 | BUSINESS IMPACT ANALYSIS (BIA)

- **What is a Business Impact Analysis?**
  The business impact analysis predicts the consequences of disruptions of business functions (utilizing information gained from the HVA) and processes (internal and external to the health center) and gathers information needed to develop recovery strategies. The BIA is a detailed functional study of the business processes, department by department.

- **Critical and Non-Critical Business Processes**
  Each department's processes are then analyzed to give the team a complete picture of health center critical and non-critical operations.
  - *Critical Processes* are essential functions that are important to the mission of the health center and must be maintained during an emergency event to keep the health center going; consider essential, mission-critical functions, and legal & regulatory requirements (an example of a critical function is patient registration or patient triage)
  - *Non-Critical Processes* play an important function to the organization but are not essential during an emergency event to keep the health center open (an example of a non-critical process is scheduling routine visits)

- **Critical Process Dependencies**
  - During a BIA, the critical process dependencies or supportive functions are also identified; these are categorized as *staff, stuff, systems, and space*

- **Recovery Time**
  - Recovery time for the critical functions is also determined; recovery time is the length of time that a critical process can be down before it begins to have a significant impact on health center operations

- **Impact Score**
  - The *impact score* is how significant the disruptions to critical and non-critical processes will be, on a scale of 1 (low) to 3 (high).

- **Example: Patient Triage**
  Patient triage is a critical process and it's dependent on *staff* (triage employees), *stuff*/supplies (medical supplies & equipment), *systems* (paper/electronic/computer/cloud-based information and communication you use to do triage), and *space* (triage area). Recovery time would need to be short, such as 0 -2 hours. Impact score would be moderate to high (2-3), depending on how much triage your center may be expected to handle.

GO DEEPER

LISTEN

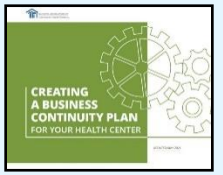
Business Impact Analysis (5 min). Amanda Cooper, MPH, Planning Specialist, Connect Consulting Services.

READ/RESOURCES

Business Impact Analysis. FEMA. 6/17/2021

ACTIVITIES

1. Complete a BIA on at least 1 essential department/functional area. BIA Tool Resources:
   - Creating a Business Continuity Plan for Your Health Center. NACHC. May 2021 (PDF).
     NACHC Business Impact Analysis Template, Appendix G (p. 24-25)
   - Business Impact Analysis Worksheet, Ready.gov (PDF)
   - Business Impact Analysis tool of your choice



2. After completing the initial BIA, develop your strategy for completing this process with all remaining health center departments/functional areas.

CHAPTER 7 | BUSINESS IMPACT ANALYSIS (BIA), cont.

- **Business Impact Analysis Report**
  The Business Impact Analysis report reflects all findings of the analyses completed during the BC Planning process:
  - Hazard Vulnerability Analysis (HVA)
  - Cybersecurity Impact Analysis (CIA)
  - Business Impact Analysis (BIA)

- **Business Impact Summary**
  Key components of the report should be summarized for quick reference:
  - Critical business processes and their priority level (e.g., low, medium, high)
    - Critical business functions that must be done immediately or in less than four (4) hours; the functions, when interrupted, may present with immediate threat to life and health.
    - 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 that need to be done within 5-7 days
  - Resources identified in the BIA process needed to continue operations.
    - 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
    - Inventory 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
  - Lists of names and contact information for 1) the business continuity and senior management teams; and 2) key health center staff, contacts, vendors, and suppliers and back up suppliers

"Identifying and evaluating the impact of disasters on business provides the basis for investment in recovery strategies as well as investment in prevention and mitigation strategies" (Business Impact Analysis, 6/17/2021, FEMA)

GO DEEPER

DISCUSS/DO
Share your planned strategy, including timeline, for completing your health center's BIAs with your executive and department leaders. Adjust as needed. Get buy-in to help assure cooperation.

ACTIVITY
After completing the remaining components of the BIA, complete the Business Impact Analysis Report and Impact Summary.

CHAPTER 8 | MITIGATION STRATEGIES

- **What are Mitigation Strategies?**
  - Mitigation strategies are aimed at protecting the health center assets and resources to prevent or minimize downtime during a disaster/disruption
  - Once the Business Impact Analysis and Summary are completed, health center processes, operations, etc. requiring a mitigation strategy will be very clear
  - The BC Planning team should seek to develop mitigation strategies for the top 3-5 identified risks; these strategies should be incorporated into your BCP

- **Mitigation Strategies to Support the Health Center May Include:**
  - Internal and external structure reinforced at the physical site
  - Ensure fire detection and suppression systems are current and operable
  - Develop redundant third-party support
  - Develop back-up systems and procedures for computers and software

- **Mitigation Strategies to Support Business Processes May Include:**
  - Procedures to incorporate appropriate inventory of critical equipment
  - Maintain adequate supplies of water, non-perishable food items, batteries, medical supplies
  - Develop offsite backup systems for data, critical software, and facilities
  - Develop disruption alternatives for key essential utilities including power, communications, data and records, and recovery of information, facility and staffing

- **Mitigation Policy**
  Your health center may also find it helpful to design a mitigation policy to identify and guide the strategy for accomplishing these activities. This policy should
  - Outline the importance of mitigation
  - Include a list of mitigation measures, the party responsible for overseeing its completion, and a timeframe for completion.

Mitigation strategies help ensure that health center assets and resources are protected, and operations downtime is held to a minimum in the midst of a disaster.

GO DEEPER

LISTEN

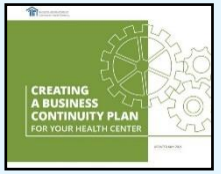
Mitigation Strategy Considerations (2:11 min). Amanda Cooper, MPH, Planning Specialist, Connect Consulting Services.

ACTIVITY

Using the template referernced below,, create your Mitigation Plan. Be sure to include all relevant health center leaders and content experts in the development and review of the plan.

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

- NACHC Mitigation Plan Template and Preparedness Activities, Appendix J (pp. 30-31)



CHAPTER 9 | RECOVERY STRATEGIES

- **What is a Recovery Strategy?**
  Recovery strategies, unlike mitigation strategies, are intended to bring the facility back to its normal operating state as quickly as possible following a disaster. Recovery strategies are typically developed in response to the identified risks likely to impact your facility.

- **Process for Developing Recovery Strategies**
  - Determine maximum tolerable downtime
  - Identify recovery strategies and courses of action
    - Determine how long a critical function can be down before it impacts operations
    - Identify recovery strategies and courses of action
    - Determine and document reimbursement and cost recovery strategies (e.g., FEMA reimbursement)

- **Disruption Categories**
  - Disruptions are likely to fall into one or more of the following categories:
    - Facility
    - Equipment
    - Staff
    - Technology
  - Procedures developed for the disruptions should cover most situations your health center may encounter
  - Develop inventories and provide contact and other important information for each category, 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

The goal of recovery strategy is to get the health center back to "normal" functioning, i.e., pre-disaster, as soon as possible.

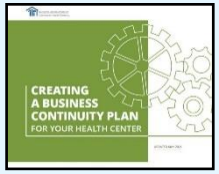
GO DEEPER

LISTEN

Recovery Strategy Overview (2:14 min). Amanda Cooper, MPH, Planning Specialist, Connect Consulting Services.

READ/RESOURCES

Familiarize yourself with these NACHC resources related to Recovery Strategies:



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

- Business Interruption Insurance, Appendix L (p. 37)
- Equipment Inventory, Appendix N (p. 41)
- Alternate Location Supplies Checklist, Appendix P (p. 43-44
- Key Contacts, Vendors, and Supplies, Appendix Q (p. 45-47)
- Cash Projections, Appendix R (p. 48)
- Mutual Aid Memorandum of Understanding, Appendix S (pp.49-56)

ACTIVITY

With the top 3-5 disruptors to your health center in mind, develop your Recovery Strategies and include as part of your BCP.

CHAPTER 10 | IMPLEMENTATION & SUSTAINABILITY

- **How Do I Implement and Sustain the Health Center's BCP?**
  At this stage of the BC planning process, the majority of the data gathering, analyses and general strategies for managing your health center through disasters has been completed. Now it's time to think about implementing and sustaining the BCP. Implementation of the preparedness program includes identifying and assessing resources, writing plans, developing a system to manage incidents and training employees so they can execute plans. These processes include the following components.

- **Composition and Role of the Ongoing BC Team**
  - The ongoing BC Team is charged with executing and sustaining the BCP completed by the BC Planning Team; the membership of these two teams do not necessarily need to be the same
  - The BC Team should be multidisciplinary, representing the major functions and processes of the health center
  - The team should have a designated BCP "Champion" either from or reporting directly to senior leadership; this will help ensure organizational focus on the plan implementation and ongoing improvement

- **Leadership Orders of Success/Delegations of Authority**
  - Continuity of leadership during an emergency is critical to ensure continuity of essential functions
  - Establish and maintain Orders of Succession in advance for key leadership and business continuity staff in the event that they are not available to fulfill their roles
  - 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

GO DEEPER

READ/RESOURCES

Crisis Communication Plan. FEMA. Helpful information on what to communicate, to whom, messaging, bi-directional communication, and resources.

Business Continuity Planning Suite (FEMA). This is an interactive software package with a comprehensive array of resources for developing your business continuity plan, including training, drills, communication.

Healthcare Business Continuity Management and Disaster Recovery— No Longer an Afterthought in Today's World. 2019. Association of Healthcare Internal Auditors (AHIA) and Crowe.

ACTIVITIES

1. Creating Your Health Center BC Sustainability Plan.
   Using the NACHC template or template of your choice for developing a Sustainability Plan, determine your plan for training, drills, debrief and policy review after a disaster, incident management and other aspects of sustaining the BCP. Be sure to review existing related health center policies to avoid duplication or competing messages. Suggested resources include:
   Creating a Business Continuity Plan for Your Health Center. NACHC. May 2021 (PDF).

   - Continuity of Leadership/Orders of Succession, p. 13
   - Emergency Communications Policy and Procedures, Appendix H (pp. 26-29)
   - Staff Training and Exercise Plan, Appendix K (pp. 32-36)
   - Transition Schedule Template, Appendix O (p. 42)
   - Incident Response and Management Team, and Command Center Considerations, Appendix M (pp. 39-40)

CHAPTER 10 | IMPLEMENTATION & SUSTAINABILITY, cont.

- **Emergency/Crisis Communications Plan & Policies**
  - During an emergency, the facility's incident management team will utilize various methods to communicate with key stakeholders, including staff, patients, contractors and other entities, vendors, 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

- **Staff Training and BC Exercises Plan**
  - The staff training and exercises plan delineates the health center's policy and resources committed to ensuring that all team members are prepared for action in the event of a disaster
  - This plan should include:
    - Schedule for staff training during the orientation period and annually
    - Methods for training staff and assuring competency
    - Delineation of the general methods and "exercises" or "drills" to be used to study and improve upon the BCP
    - Procedures for debriefing staff after the exercises

- **Incident Command System and Incident Management Team**
  - The Incident Command System (ICS) structure allows organizations to respond to any emergency in a planned, organized, and efficient way, through to recovery
  - 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: 1) operations, 2) planning, 3) logistics, and 4) finance/administration
  - The IMT also includes additional staff who fill supporting roles in public information, safety, and interagency coordination

GO DEEPER, cont.

ACTIVITIES, cont.

2. Conducting BC Training Exercises**.**
   In this activity, you will conduct tabletop drills/exercises for staff training purposes. Try them out with the BC Planning team or another group of staff. This exercise is to help you become familiar with the process and some of the resources readily available to assist you in creating a customized training exercise.

   Download the Business Continuity Suite (FEMA).

   Within the documents located in the folder you will find the following resources that will get you started on your way to conducting BCP exercises and training others to assist you:
   - BCP Exercise Planner Instructions
   - BCP Facilitator & Evaluator Handbook
   - BCP Participant Feedback Form
   - BCP Situation Manual
   - BCP Presentation

CHAPTER 10 | IMPLEMENTATION & SUSTAINABILITY, cont.	GO DEEPER, cont.	
• **Business Continuity Policy** Finally, the health center must make a formal commitment to the BCP to sustain the work of the BC Planning Team. Ideally, this policy should include: ○ Identification of the role responsible for ensuring the BCP is implemented ○ Requirement for active BC Planning Team and the required departments/functions that should be represented on the team ○ Guidelines for frequency of review of the BCP ○ Policy for BC training, drills/exercises ○ Staff training procedures: how staff will be trained on the plan including who is responsible, frequency and training topics by staff role/position ○ Debriefing/process-improvement procedures after a disaster ○ Documenting a schedule of BCP activities in the policy that is integrated into ongoing operations will help ensure that it is maintained • **Tracking Changes to the BCP and Policy** ○ BC Planning Teams should track all changes to the BCP. Two suggested methods include: ▪ Maintain a revision page in the BCP with a running list of updates ▪ At the bottom of each policy, insert a space titled "Last Updated" and record the date of the last revision  ***Focusing on the activities required to ensure the BCP is understood, utilized and effective will help create good outcomes and ongoing utilization and improvement of the plan.***		

<table>
<tr><th>CHAPTER 11 | EXECUTIVE SUMMARY & PUTTING IT ALL TOGETHER</th><th colspan="2">GO DEEPER</th></tr>
<tr><td rowspan="2">

- **The Executive Summary is the last step in writing the BCP and is placed at the beginning of the planning document.**
  The executive summary includes key information the provides the rationale and evidence supporting its adoption and implementation.
  - The BCP purpose
  - 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 for BCPs that are specific to the health center can support buy-in. Consider entering a summary of your business case in this section. Some general statistics to consider including are:
    - 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 (estimate for your health center, if possible)
    - 50% of businesses which sustain interruptions of a week or more due to problems at the primary site never recover

</td><td> 
</td><td>

READ/RESOURCES

Business Continuity Planning Suite (FEMA). This is an interactive software package with a comprehensive array of resources for developing your business continuity plan.

</td></tr>
<tr><td> 
</td><td>

ACTIVITY

Taking into consideration all of the information that has been collected and analyzed in the BC Planning process, it's time to write an executive summary!

Creating a Business Continuity Plan for Your Health Center. NACHC. May 2021 (PDF).
- Executive Summary Template, p. 17

</td></tr>
</table>

CHAPTER 12 | FREQUENTLY ASKED QUESTIONS

QUESTIONS	ANSWERS
1. ***Do you recommend addressing specific vulnerabilities (e.g., fire, flood, etc.) or categories of vulnerabilities (e.g., physical or building damage) in the BCP?***	Early in the process the top three to five threats identified by the health center help to focus the BC planning efforts. When doing the HVA, you want to consider everything that is *likely* to happen, so yes, you would need to look at vulnerabilities individually rather than categorically.
2. How might BCPs change post-COVID?	BCPs are intended to cover a broad range of disasters, most of which are relatively short-lived. In the case of a pandemic, like COVID, a longer-term strategy may be in order. Consider developing a pandemic centered BCP or include longer term pandemics in the HVA so that they are addressed adequately. Be sure to integrate successful strategies used by your health center during COVID into your pandemic BCP. Your pandemic response plan will overlap with your BCP.
3. *How should health centers factor in individual site shutdowns in their BCP?*	Think of each site as an asset with personnel, supplies, pharmaceuticals, i.e., "stuff." The BCP should address relocation/repurposing of the "stuff" associated with locations that are closing to help maintain as much volume in operations as possible. Part of the BC planning process is to consider alternatives to "space" or location of the operations. Mobile units may serve a really big assets during these processes.
4. What resources are available to help us put the comprehensive plan together?	The NACHC Creating a Business Continuity Plan resource guide and this training program have many resources/templates for helping you develop the plan. In addition, your PCAs, healthcare coalitions, HIMMS local chapters, state Emergency Management Assistance Compact, etc., may also have BCP and emergency response resources.

CHAPTER 13 | KNOWLEDGE CHECK: CREATING A BUSINESS CONTINUITY PLAN

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. The role of the health center board of directors in the BC Planning process is to: (select the best answer):
    A. Select the BC Planning leader
    B. Write the BCP
    C. Evaluate the BC Planning team
    D. Ensure the health center maintains an effective BCP
    E. All of the above
2. A Hazard Vulnerability Analysis (HVA) is a study of the disasters that are ____ likely to occur at the health center. (fill in the blank).
    A. Moderately
    B. Least
    C. Most
    D. Never
3. The components of HVAs include (select all that apply):
    A. Identifying risks
    B. Determine information value
    C. Identifying any control weaknesses and/or single points of failure
    D. Identifying the top 3-5 vulnerabilities for which mitigation plans should be developed
    E. Critical Business Processes
    F. Conduct HVA annually
4. The role of the BC Planning Team is to (select the best answer)
    A. Direct the health center's response during an actual disaster
    B. Lead the development of the health center's BCP
    C. Develop and facilitate staff training on the BCP policies and protocols
    D. Complete independent risk assessments on each health center department
    E. Conduct practice drills
    F. B, C and E only
5. The Business Impact Analysis (BIA) is intended to bring the facility back to its normal operating state as quickly as possible. True/False
6. Mitigation strategies may include (select the best answer):
    A. Internal and external structure reinforced at the physical site
    B. Ensure fire detection and suppression systems are current and operable
    C. Develop redundant third-party support
    D. Develop back-up systems and procedures for computers and software
    E. All of the above
7. Critical process dependencies can be categorized as (select the best answer):
    A. staff, stuff, systems, and space
    B. space, speed, systems, and storage
    C. systems, space, signage, stuff
8. The BC Planning team is responsible for developing an effective training plan for health center staff. True/False
9. Mitigation strategies are aimed at protecting the health center assets and resources to prevent or minimize downtime during a disaster/disruption. True/False
10. Which of the following are NOT major components of the cybersecurity plan? (select all that apply)
    A. Identify Critical Systems Assets
    B. Vacation/PTO time analysis
    C. Identify Threats to Cybersecurity
    D. Identify Vulnerabilities
    E. Inventory of staff members' personal smartphones/technologies
    F. Develop Cybersecurity Action Plan

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

CHAPTER 14 | PREPARING FOR MODULE 3: ENSURING A HUMAN RESOURCES STRATEGY

OVERVIEW	PREPARING FOR MODULE 3	
The next module is focused on providing you with information on the best human resource strategies to implement during a disruption of health center operations due to disaster. Understanding these principles and practices will help to enrich your BCP. Topics include providing support through wrap-around services, best practices for staff management during an emergency and key incident response team roles. Finally, we will review what it means to have a successful succession plan in place as well as a brief overview of the practice of telecommuting.		**REFLECT ON…** 1. What concerns will health center staff have in the event of a disaster? How might their concerns vary based on the type or severity of the disaster? 2. What happens when key team members are unable to report to work? Do we have a succession plan? 3. Is our health center ready to shift a significant portion of our services to telemedicine? Is our patient population ready? What is needed to make a telemedicine strategy more successful?

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