NATIONAL ASSOCIATION OF Community Health Centers®

Business Continuity Institute

Session 2: Creating a Business Continuity Plan

Wednesday, May 12, 2021

THE NACHC MISSION

America's Voice for Community Health Care

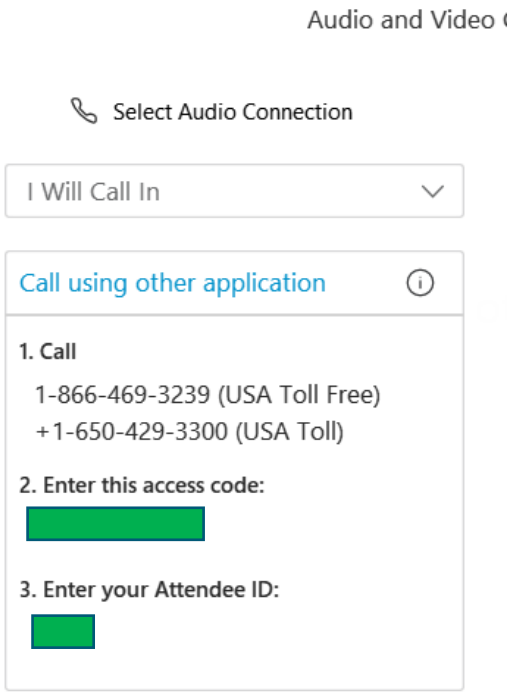
The National Association of Community Health Centers (NACHC) was founded in 1971 to promote efficient, high quality, comprehensive health care that is accessible, culturally and linguistically competent, community directed, and patient centered for all.

NATIONAL ASSOCIATION OF Community Health Centers®

AUDIO CONNECTIONS

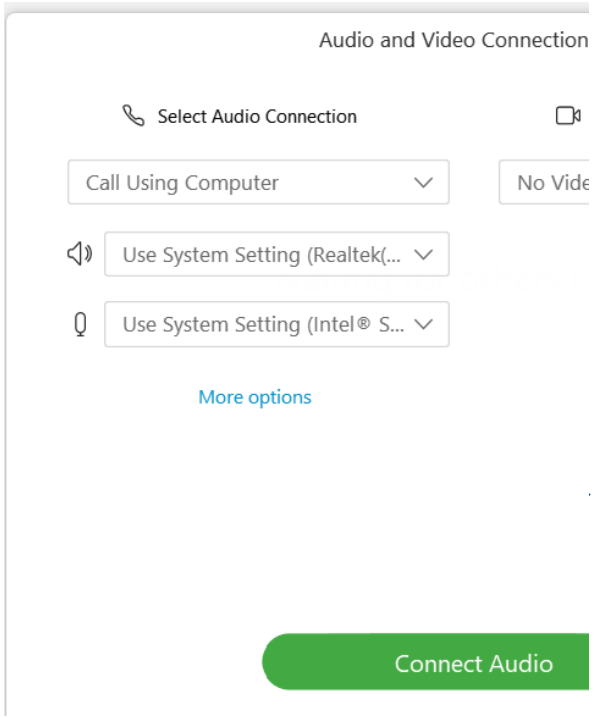
Option 1: "I Will Call In"

Follow the unique 3-step process on your screen

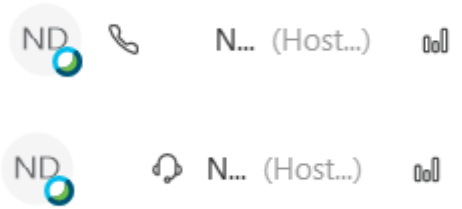


Option 2: "Call Using Computer "

You must have computer speakers and microphone



After connecting, if you don't see a phone/headset icon next to your name, please attempt to connect your audio again!

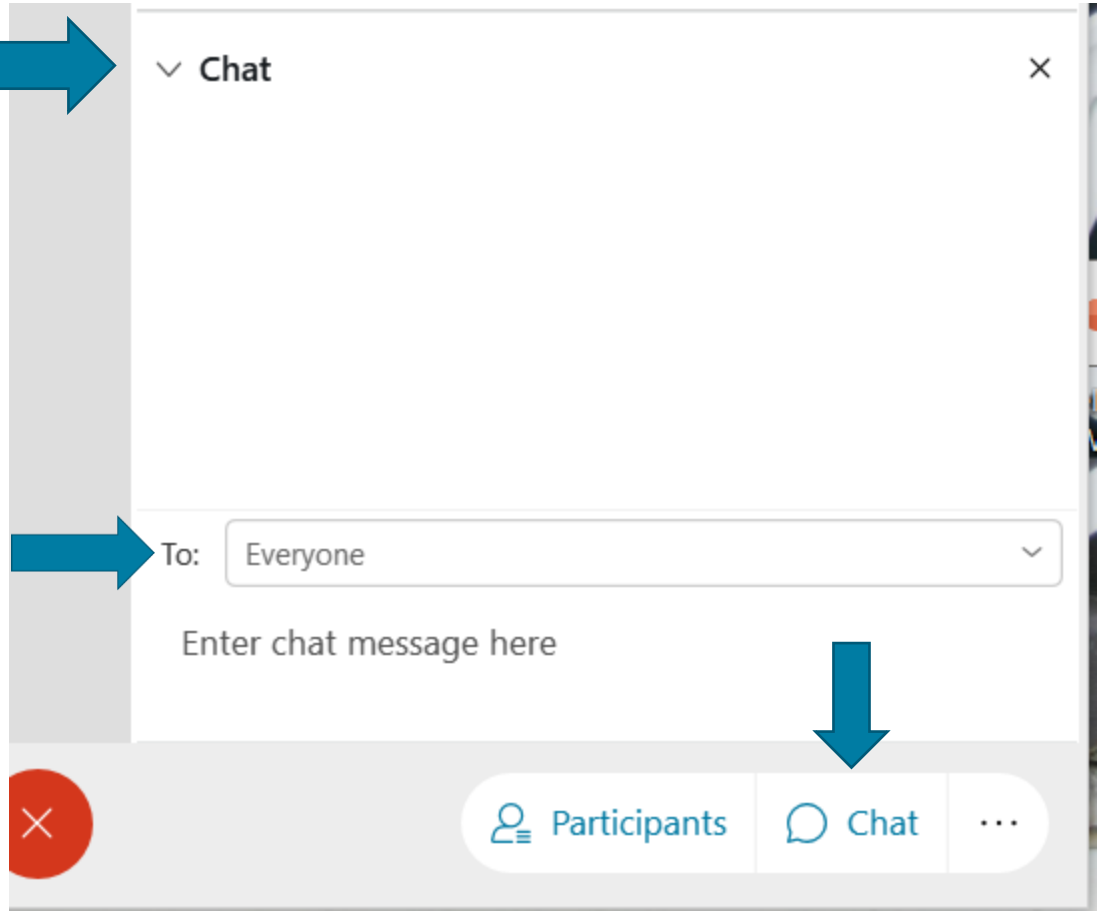


ASKING QUESTIONS VIA CHAT BOX

1. **The chat feature** is available to ask questions or make comments anytime.

2. **Click the chat button** at the bottom of the WebEx window to open the chat box on the bottom righthand side of the window.

3. **Choose "Everyone",** as appropriate.
   - Type your question.
   - Click ***"Enter"*** to send your question.



Friendly Reminders

- Today's Event is being **RECORDED**
- All attendee lines have been **MUTED**
- The **CHAT BOX** is open for the duration of this event
- Questions from the **CHAT BOX** will be answered after the presentation is completed or in our FAQ document
- You'll be presented with a brief **SURVEY** after the event is completed

Meet our presenters

Amanda Cooper, MPH

Planning Specialist
Connect Consulting Services

Anthony L. Hurley, MEP, CPP®, PCI®, PSP®, CPD

Director, Emergency Management
Connect Consulting Services

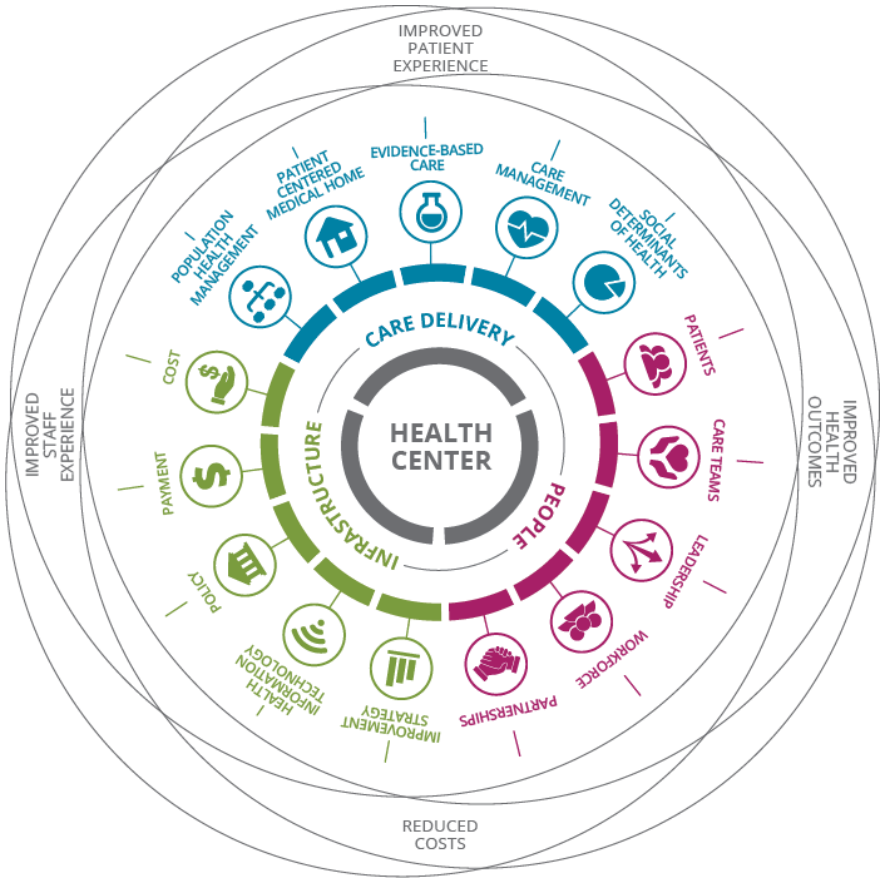
Nora O'Brien, MPA, CEM

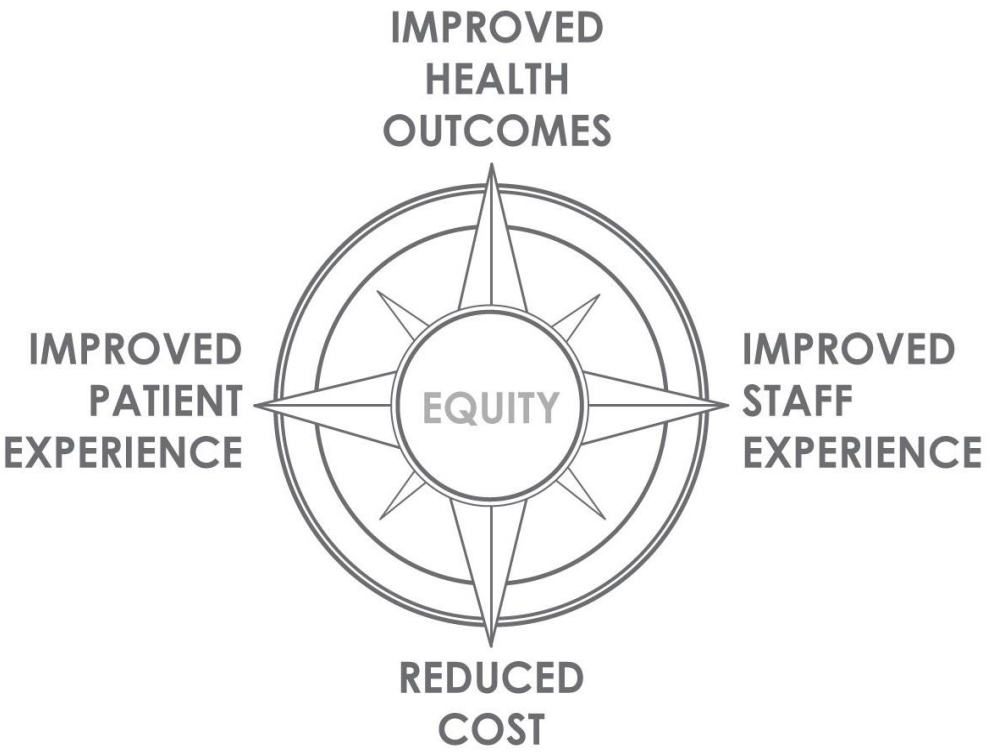
Founder and CEO
Connect Consulting Services

Gervean Williams

Director Health Center
Financial Training
Training and Technical Assistance
NACHC

NACHC's Value Transformation Framework

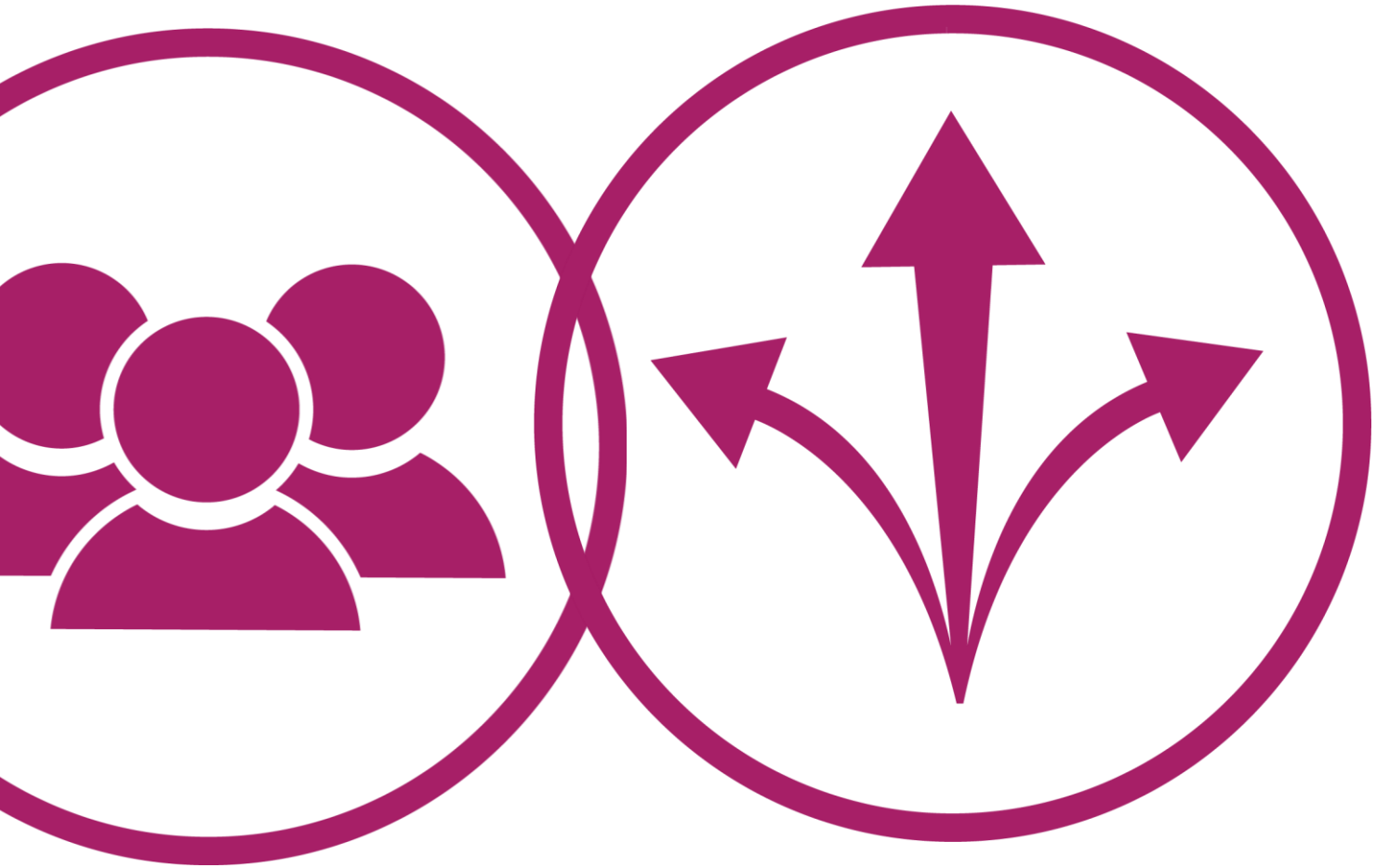




https://www.nachc.org/clinic matters/value-transformatio framework/

Value Transformation Framework

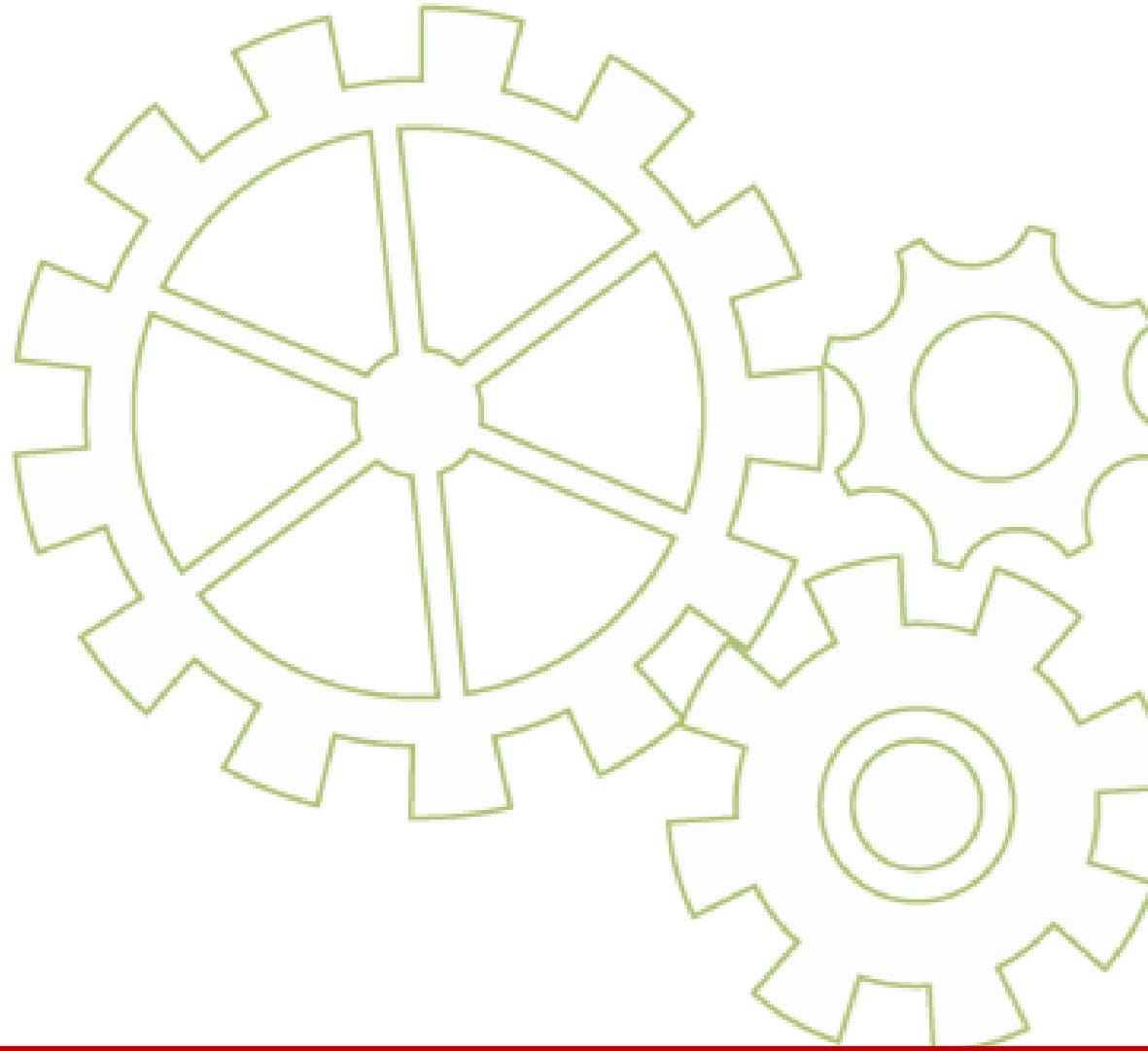
CHANGE AREAS



WORKFORCE **LEADERSHIP**

BUSINESS CONTINUITY INSTITUTE

CREATING A BUSINESS CONTINUITY PLAN



OBJECTIVES

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

AGENDA

- Key components of a Business Continuity Plan (BCP)
- Using BCP tools
- Cybersecurity for Healthcare
- Cybersecurity Impact Analysis

KEY COMPONENTS OF A BCP

BCP—DETAILS AND KEY COMPONENTS

- Executive Support
- BCP Planning Team
- Hazard Vulnerability Analysis
- Business Impact Analysis
- Business Impact Analysis Summary
- Mitigation Strategy
- Recovery Strategy
- Training, Drills and Ongoing Maintenance

KEY COMPONENT— EXECUTIVE SUPPORT

Senior management team is responsible for overseeing the process

- Establishing policy
- Allocating personnel and financial resources
- Ensuring the BCP is reviewed and approved annually
- Ensuring employees are trained

KEY COMPONENT— PLANNING TEAM

Core team is responsible for developing the plan

Team should include:

- Appointed BCP manager
- C-Suite or executive team member
- Safety Officer
- HR
- Public Information
- Finance
- Legal
- Facilities

KEY COMPONENT— HAZARD VULNERABILITY ANALYSIS

Risk assessment to identify and minimize key risks/threats

- Control weaknesses and/or points of failure
- Mitigation/corrective(s) measure to address
- Select, implement, and document mitigation/corrective measure(s)
- Ensure facility personnel awareness of risks

KEY COMPONENT— BUSINESS IMPACT ANALYSIS

Detailed study of all the business processes within the organization, department by department:

- Critical processes—essential business functions
- Non-critical processes—important functions, but not critical
- Dependencies (staff, stuff, systems, space)
- Recovery time
- Business impact score

KEY COMPONENT— MITIGATION STRATEGY

Strategy to address identified risks

- Critical equipment inventory
- Maintain adequate supplies of water, non-perishable food items, batteries, medical supplies
- Develop offsite backup systems for data, critical software & facilities
- Develop disruption alternatives for key essential utilities

KEY COMPONENT— RECOVERY STRATEGY

Developed for identified risks

- Determine maximum tolerable downtime
- Identify recovery strategies and courses of action
- Determine and document reimbursement and cost recovery strategies

KEY COMPONENT— TRAINING, DRILLS, AND MAINTENANCE

Process for implementation and annual maintenance of BCP

- Designate facility lead
- Identify review frequency of plan
- Determine staff training process
- Determine how the plan will be incorporated into drills/exercises and the frequency of testing

Does your health center have a business continuity plan?

I don't know.	**A**
Yes, but I have not seen it.	**B**
Yes, and I have seen it.	**C**
No	**D**

USING BCP TOOLS

BUSINESS CONTINUITY METHOD TOOLS

TRADITIONAL METHOD

Process to have each department complete a BIA worksheet

A member of the BCP Team interviews each department individually to validate the worksheet information

COMBINATION METHOD

A combination of approaches may be useful and more effective for your facility to initially develop and/or update BCPs

GROUP METHOD

Representatives from similar departments are brought together in workshops to complete the worksheet or BCP template. May save time and provide more details with the group thinking together

DELEGATIONS OF AUTHORITY

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. Incident Commander 2. Chief Nursing Officer 3. Director of Nursing

STAFFING ANALYSIS

Position Title	Essential Service	Remote Work Capability	FTEs Required during Normal Conditions	Minimum FTEs Required during Crisis	FTE Available for Reassignment
Director	Administration	Y	1	1	0
Manager	Administration	Y	1	1	1
Admin Assistant	Administration	Y	1	1	0
Charge Nurse	Patient Care	N	2	1	1
Staff RN	Patient Care	N	2	0	2
LVN	Patient Care	N	6	3	3

ESSENTIAL BUSINESS FUNCTIONS

Department	Essential Function	Maximum Tolerable Downtime
Finance	Payroll	48 hours
IT	Server updates	4 hours
Clinic	Scheduling	24 hours

MAXIMUM TOLERABLE DOWN TIME

Essential Function	Dependency	Department Responsible	Actions if Dependency is Unavailable	Maximum Tolerable Downtime
Lights	Electricity	Facilities	Use flashlights, open curtains	0 - 2 hours
EMR, orders, lab results	Computers	IT	Implement downtime procedures	2 - 12 hours
O2	Medical gases	Facilities	Portable tanks	2 - 12 hours
Desk Phones	Communication Devices	Telecommunications	Handheld radios, cell phones	12 - 24 hours

ESSENTIAL EQUIPMENT & SUPPLIES

Description (item, brand, size, etc.)	Usual Quantity	Post Incident	Actions if Equipment is Unavailable	Maximum Tolerable Downtime
Computer (with monitor, keyboard, mouse)	10		Use downtime forms and procedures	12 hours
Desk phones	10		Handheld radios, cell phones	12 hours

ESSENTIAL VITAL RECORDS

Vital Records	Location			
ESSENTIAL FUNCTION	ELECTRONIC COPY	HARD COPY	MOBILE COPY	REMOTE BACK-UP
Policy and Procedures (SOPs)				
Emergency Operations Plan				
Admission Records				
Licenses (RN, LVN, MD)				
Timecards				

Vendor Resources Contact List

Service	Company	Point of Contact	Emergency Phone Number	Emergency Contract?	Maximum Tolerable Downtime
Gas	PG&E				
Consumable medical supplies	Omnia Health				
Medical equipment maintenance	MedShare				

PHASES OF RECONSTITUTION

- Recovery - resume normal operations in the primary operating space
- The four key phases of reconstitution:

PROJECT TOGO

Yukon Kuskokwim Health—Alaska

CYBERSECURITY FOR HEALTHCARE

CYBERSECURITY FOR HEALTHCARE

- Healthcare experience significant breaches with malicious criminals responsible for most incidents.
- Some of these sectors are more appealing to cybercriminals because they collect financial and medical data
- All businesses that use networks can be targeted for customer data, corporate espionage, or customer attacks

OVERVIEW OF CYBERSECURITY

Practice of defending equipment, systems, and data

- Network security—secures a computer network
- Application security—software and devices free of threats
- Information security—protects the integrity and privacy of data
- Operational security—handles and protects data assets

SAFE PRACTICES FROM EMPLOYEES

- Define data policies and procedures
- Conduct cybersecurity awareness trainings
- Strong network and system passwords
- Multiple authentication methods for computers and networks
- Prohibit transmittal of PHI via unencrypted public networks (i.e., free Wi-Fi hotspots)

* Protect Healthcare and Public Health Infrastructure :https://www.phe.gov/Preparedness/planning/cip/Pages/protect.aspx

CYBERSECURITY IMPACT ANALYSIS

Tool that is used to answer the following questions:

- What information assets may be affected by an attack?
- What are the current and relevant threats?
- What are the internal and external vulnerabilities?
- What security attacks could affect daily operations?
- What level of risk are we comfortable taking?

STEP 1. DEFINE INFORMATION VALUE

- Will your health center face penalties if information is exposed?
- How valuable is this information to outsiders?
- If information is lost, how easily could it be recreated? Will the loss of information negatively impact revenue and/or profitability?
- If information is lost, would your day-to-day operations be impacted?

STEP 2. CRITICAL SYSTEMS ASSETS

- All devices including computers, tablets, routers, printers, etc.
- How devices are used and how they connect
- Departments and individuals with access to each device
- Network resources not physically located at the health center (e.g., data stored in the cloud)

STEP 3. IDENTIFY THREATS TO CYBERSECURITY

- Natural disasters – fires, floods, etc.
- System failure – software, hardware
- Human error – malware, phishing, social engineering

STEP 4. IDENTIFY VULNERABILITIES

- Weakness that can be exploited
- Intention of breaching security that can harm your health center
- Implementing proven best practices reduces vulnerabilities

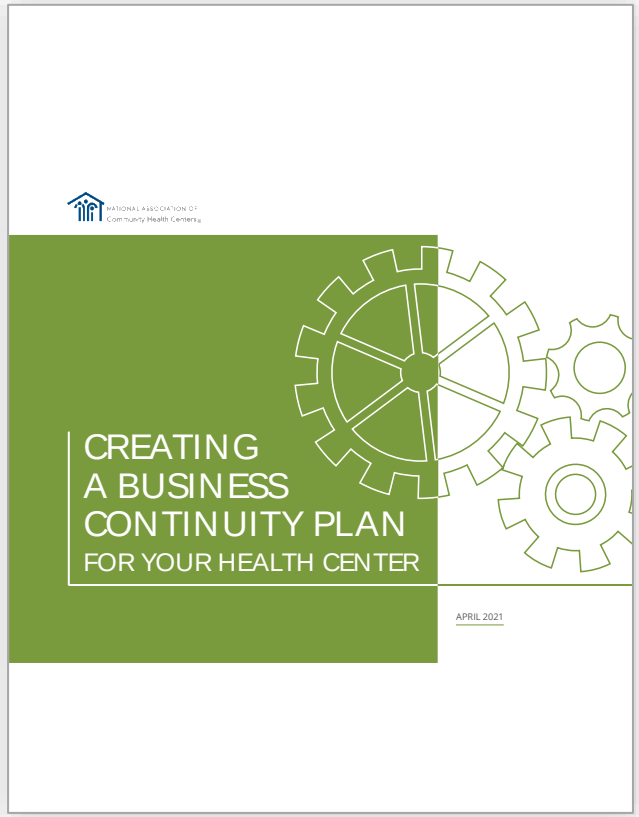
STEP 5. DEVELOP A SET OF CONTROLS

- Set up and configure a firewall
- Segregate networks
- Create password policy for all employees and devices
- Install anti-malware and anti-ransomware tools
- Use multifactor authentication for users accessing health center systems
- Use vendor risk management software

STEP 6. DEVELOP CYBERSECURITY ACTION PLAN

- Work with a vendor or use tools that can assist in detecting threats
- Conduct annual cybersecurity risk analysis
- Test your plan annually

RESOURCE



CREATING A BUSINESS CONTINUITY PLAN FOR YOUR HEALTH CENTER

https://www.nachc.org/clinical-matters/current-projects/building-capacity-of-community-health-centers-to-respond-to-covid-19/#crisis-business-continuity

CONNECT WITH US!

Connect Consulting Services
Emergency Management and
Business Continuity Planning

Office: 916-758-3220
Fax: 916-750-2882
Email: Connect@ConnectConsulting.biz

Schedule a Call with Connect Consulting Team

About Connect Consulting

Nora O'Brien, MPA, CEM
Founder and CEO

Office: 916-758-3220
Mobile: 916-806-7361
Email: Nora@ConnectConsulting.biz

Schedule a Call with Nora O'Brien

Nora O'Brien Bio

Amanda Cooper, MPH, CADAC/P
Planning Specialist

Office: 916-758-3220
Mobile: 916-541-7937
Email: Amanda@ConnectConsulting.biz

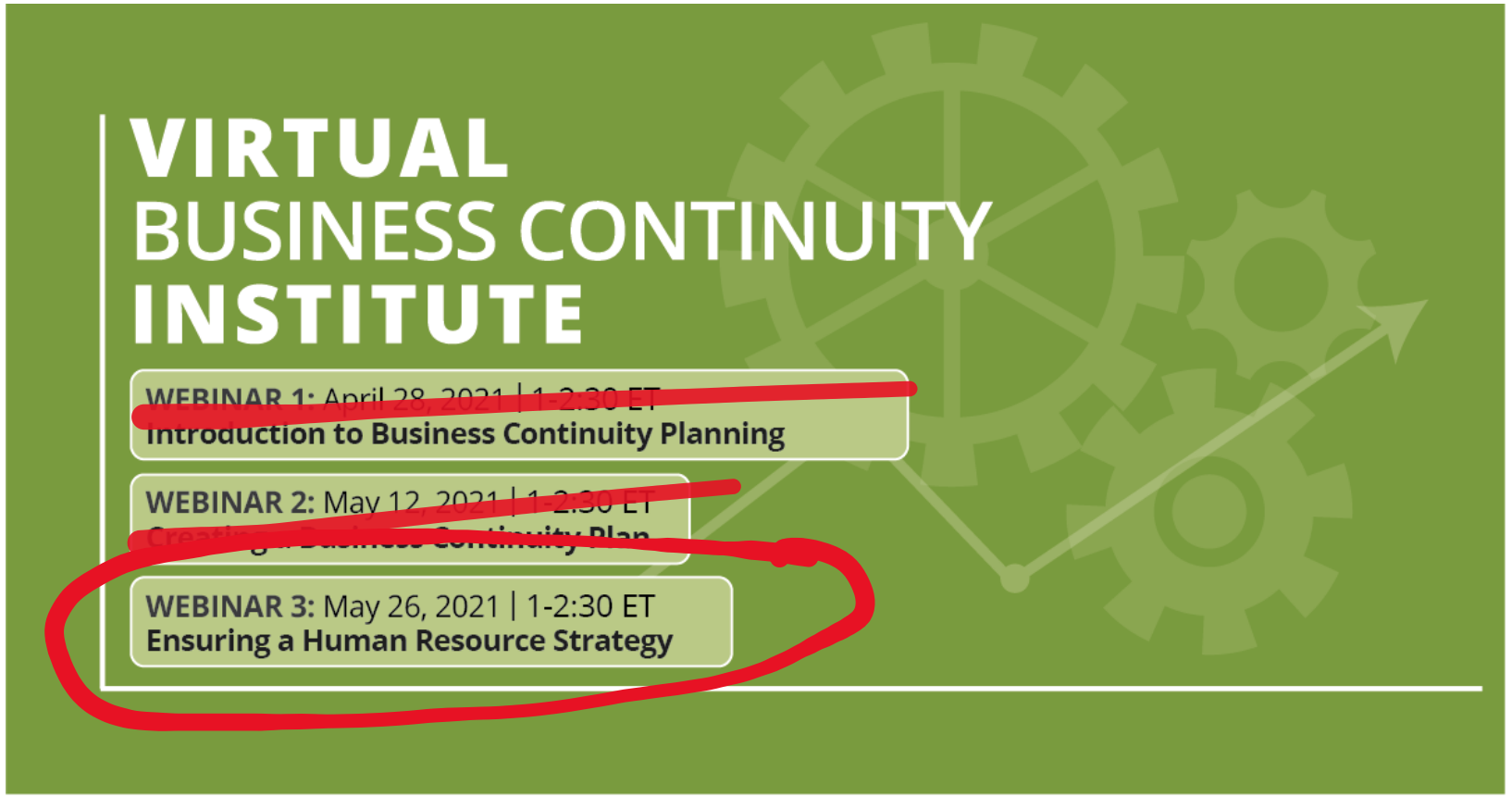
Schedule a Call with Connect Consulting Team

Amanda Cooper Bio

Thank you!

SAVE THE DATE

Only one session remaining!



FOLLOW US

Twitter.com/NACHC

Facebook.com/nachc

Instagram.com/nachc

Linkedin.com/company/nachc

YouTube.com/user/nachcmedia

THANK YOU TO ALL COMMUNITY HEALTH CENTERS

#ThankYouCHCs