NYS Health Center Controlled Network

CHCANYS

CHCANYS EM Team

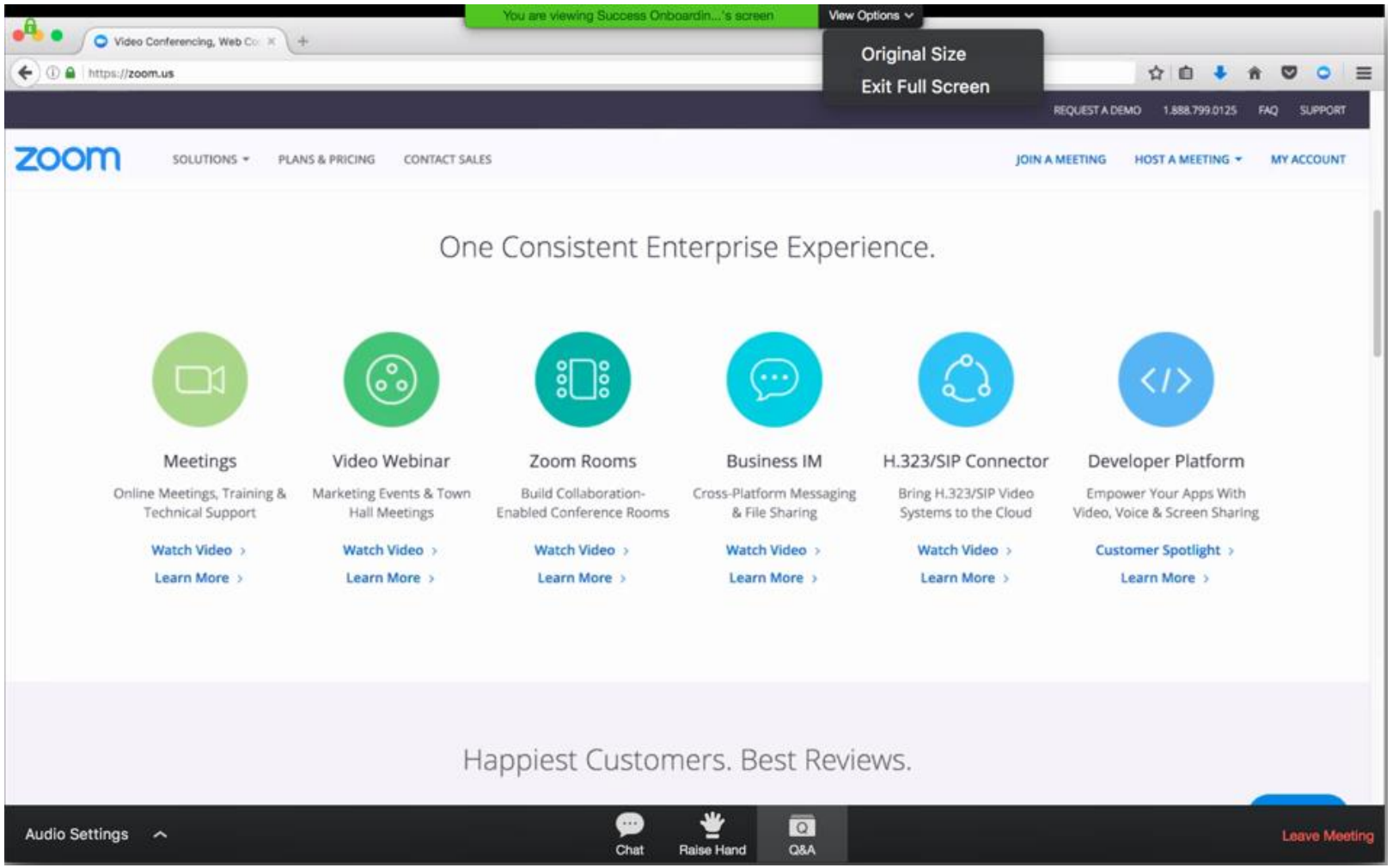
Cybersecurity Webinar Series

Part I - Emergency Management Planning for Cybersecurity

February 12, 2020

CHCANYS

Q&A


You are viewing Success Onboardin...'s screen
View Options
Original Size
Exit Full Screen
Video Conferencing, Web Co
https://zoom.us
REQUEST A DEMO
1.888.799.0125
FAQ
SUPPORT
zoom
SOLUTIONS
PLANS & PRICING
CONTACT SALES
JOIN A MEETING
HOST A MEETING
MY ACCOUNT
One Consistent Enterprise Experience.
Meetings
Online Meetings, Training & Technical Support
Watch Video
Learn More
Video Webinar
Marketing Events & Town Hall Meetings
Watch Video
Learn More
Zoom Rooms
Build Collaboration-Enabled Conference Rooms
Watch Video
Learn More
Business IM
Cross-Platform Messaging & File Sharing
Watch Video
Learn More
H.323/SIP Connector
Bring H.323/SIP Video Systems to the Cloud
Watch Video
Learn More
Developer Platform
Empower Your Apps With Video, Voice & Screen Sharing
Customer Spotlight
Learn More
Happiest Customers. Best Reviews.
Audio Settings
Chat
Raise Hand
Q&A
Leave Meeting

Disclaimer

This is a NYS Health Center Controlled Network (NYS-HCCN) Activity

A HRSA-Funded Project of the Community Health Care Association of New York State

HCCN Grant Number: H2QCS30278

Welcome

Alex Lipovtsev

Director – Health Center Support
Emergency Management

alipovtsev@chcanys.org
212-279-9686 x127

2020 HCCN Webinar Series

The webinar series consists of 3 parts with the following schedule:

Today

February 12

Part I - Emergency Management Planning for Cybersecurity

- *Introduction, general concepts of emergency management that would be important to consider for cybersecurity and protecting your data and systems.*

February 26

Part II – Cybersecurity Hazards: Threat, Assessment & Recovery

- *Focus on cybersecurity as a specific hazard, assessment of vulnerabilities, making a robust plan and recovering quickly when affected.*

March 10

Part III – Cybersecurity through the lens of Business Continuity

- *Cybersecurity activities through the prism of the general organizational business continuity planning efforts*

2020 HCCN Webinar Series

HEALTH INFORMATION TECHNOLOGY, EVALUATION, AND QUALITY CENTER

Additionally, HITEQ will host the following webinars part of this HCCN series:

March 24 Ransomware Guidance

12:00 pm – 1:00 pm

- *TO JOIN -* https://zoom.us/j/958917558?pwd=emZ2WXF1N3o2eU1YSjMzdmJ0ZFhkdz09
  Password: 290814

April 7 Cybersecurity Breach Protection and Response

11:30 am – 12:30 pm

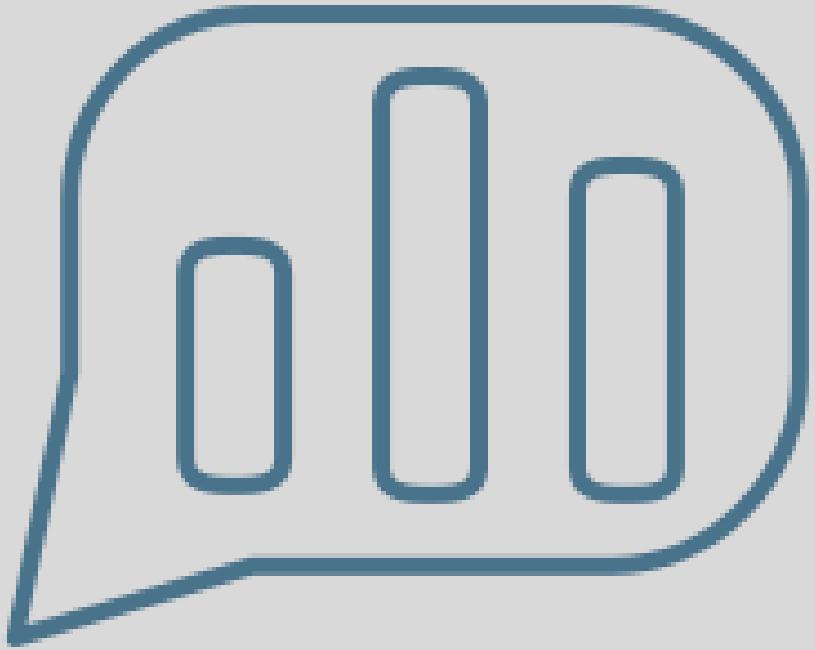
- *TO JOIN -* https://zoom.us/j/342999407?pwd=cEE4RUtMMTZ2dGRoSitRNW5Pd3Jldz09
  Password: 255076

CHCANYS

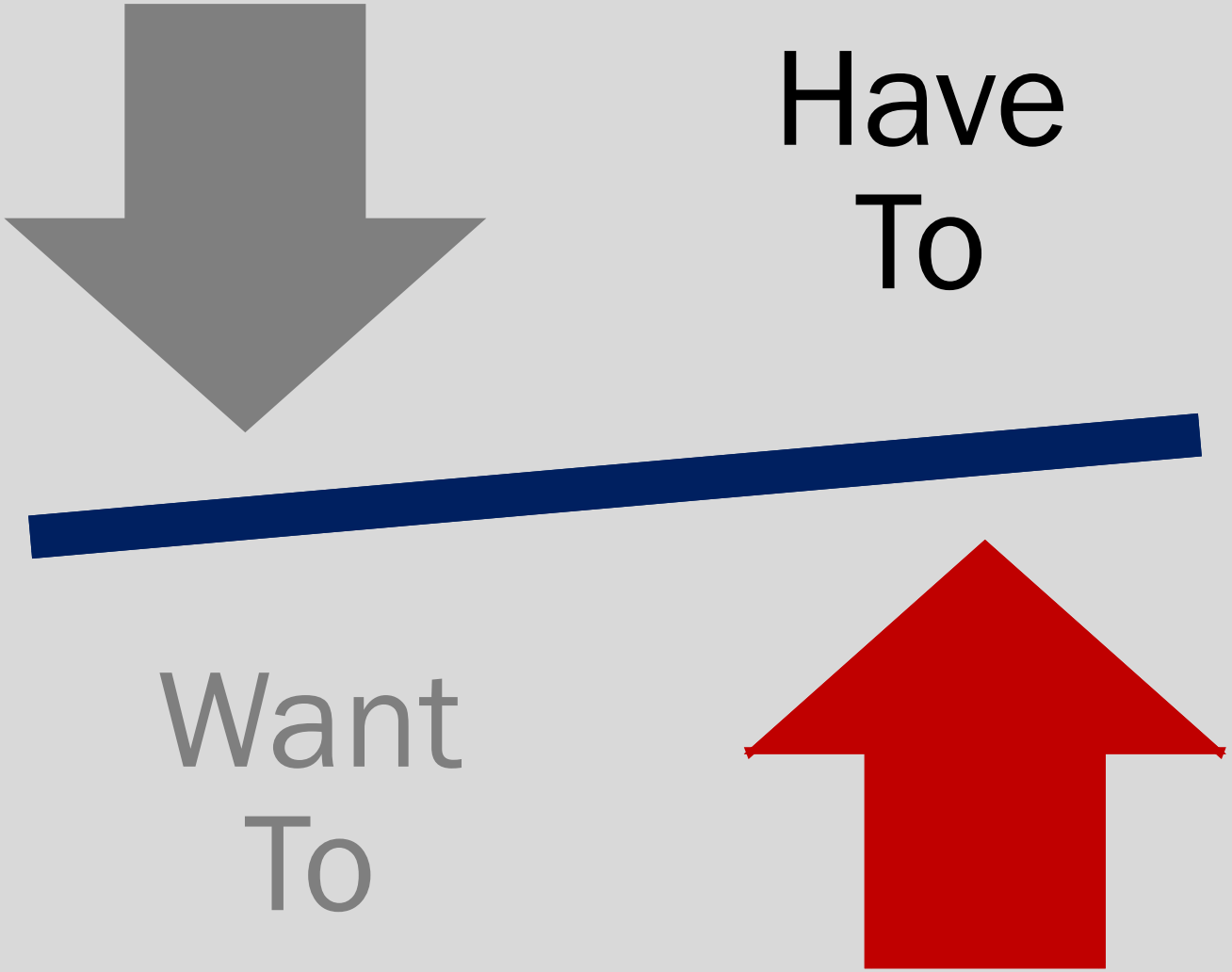
Today's Objectives

- Identify reasons for increased focus on cybersecurity
- Discuss general concepts of organizational emergency management and how cybersecurity fits in
- Understand the structure for an organizational emergency operations plan (EOP)
- Provide relevant resources

Participant Poll

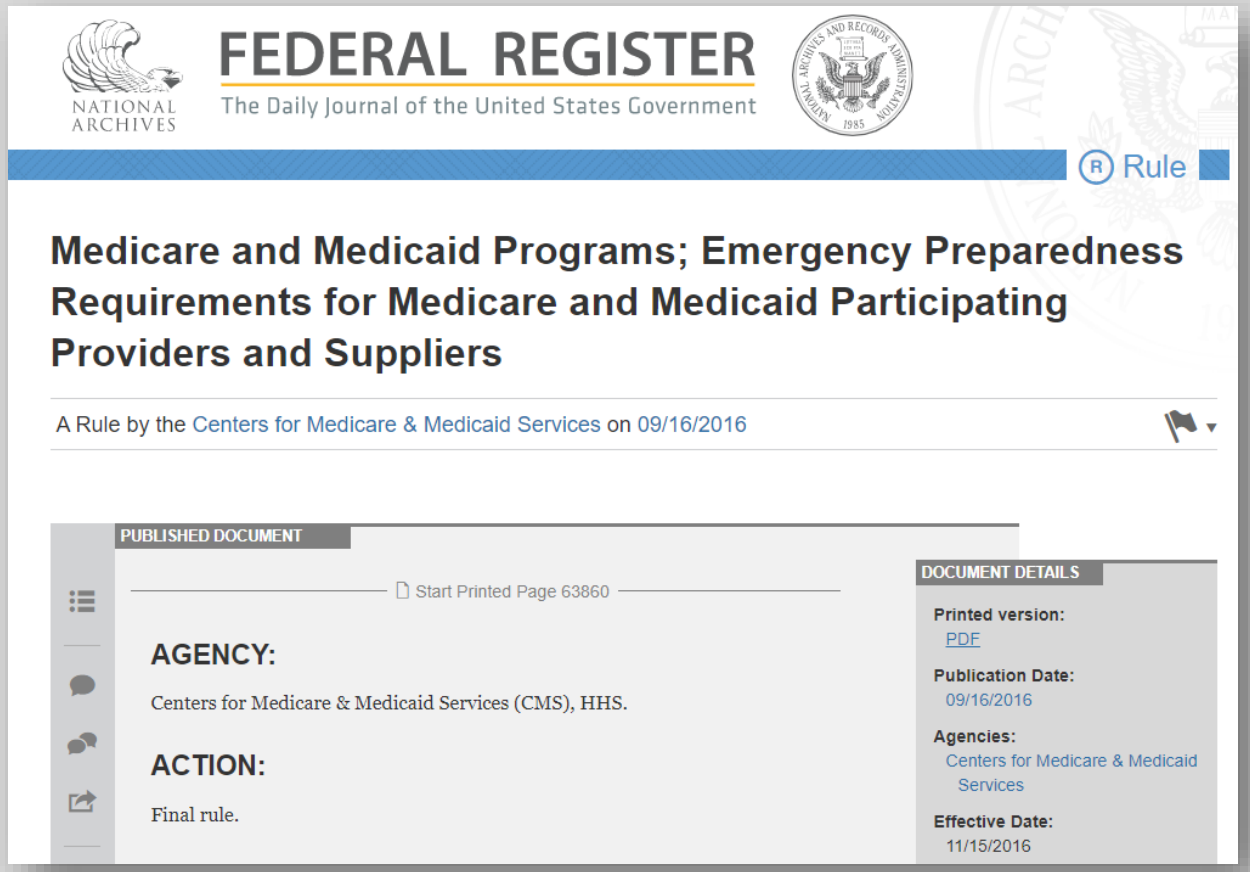


Why Worry About Cybersecurity?



CMS Emergency Preparedness Final Rule

- November 15, 2016 – *Emergency Preparedness Requirements for Medicare and Medicaid Participating Providers and Suppliers*.
- The goals of the new rule are:
  - *Increase patient safety during emergencies*
  - *Establish consistent emergency preparedness requirements across provider and supplier types*
  - *Establish a more coordinated response to natural and man-made disasters*.


NATIONAL ARCHIVES

FEDERAL REGISTER

The Daily Journal of the United States Government

Rule

Medicare and Medicaid Programs; Emergency Preparedness Requirements for Medicare and Medicaid Participating Providers and Suppliers

A Rule by the Centers for Medicare & Medicaid Services on 09/16/2016

PUBLISHED DOCUMENT

Start Printed Page 63860

AGENCY:

Centers for Medicare & Medicaid Services (CMS), HHS.

ACTION:

Final rule.

DOCUMENT DETAILS

Printed version: PDF

Publication Date: 09/16/2016

Agencies: Centers for Medicare & Medicaid Services

Effective Date: 11/15/2016

https://www.federalregister.gov/d/2016-21404/p-amd-38

Purpose of the CMS EP Final Rule

The rule establishes national emergency preparedness requirements to ensure adequate planning for both natural and man-made disasters, and coordination with Federal, state, tribal, regional, and local emergency preparedness systems.

The rule addresses the three key essentials necessary for maintaining access to health care services during emergencies:

- Safeguarding human resources
- Maintaining business continuity
- Protecting physical resources

An All-Hazards Approach

- Integrated approach to emergency preparedness that focuses on identifying hazards and developing emergency preparedness capacities and capabilities that can address those as well as a wide spectrum of emergencies or disasters.
- This approach includes preparedness for natural, man-made, and or facility emergencies that may include but is not limited to: care-related emergencies; equipment and power failures; interruptions in communications, including cyber-attacks; loss of a portion or all of a facility; and, interruptions in the normal supply of essentials, such as water and food.
- All facilities must develop an all-hazards emergency preparedness program and plan.

*Appendix Z- EP SOM February 2019

NYS Title 10 - Section 702.7 - Emergency and disaster preparedness

702.7 Emergency and disaster preparedness.

- Medical facilities shall have an acceptable written plan, rehearsed and updated at least twice a year, with procedures to be followed for the proper care of patients and employees, including the reception and treatment of mass casualty victims, in the event of an internal or external emergency or disaster arising from the interruption of normal services resulting from earthquake, tornado, flood, bomb threat, strike, interruption of utility services and similar occurrences.
- All employees are to be trained in all aspects of preparedness for any interruption of services and for any disaster.

https://regs.health.ny.gov/content/section-7027-emergency-and-disaster-preparedness

HIPAA Security Rule Requirements

- The HIPAA Security Rule requires HIPAA covered entities and business associate to identify and respond to suspect or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes. See 45 C.F.R. § 164.308(a)(6).
- The HIPAA Security Rule also requires HIPAA covered entities and business associates to establish and implement contingency plans, including data backup plans, disaster recovery plans, and emergency mode operation plans. See 45 C.F.R. § 164.308(a)(7).

https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/adminsafeguards.pdf?language=es

HIPAA Security Rule

The HIPAA Security Rule requires covered entities to maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting e-PHI. Specifically, covered entities must:

- Ensure the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain or transmit;
- Identify and protect against reasonably anticipated threats to the security or integrity of the information;
- Protect against reasonably anticipated, impermissible uses or disclosures; and
- Ensure compliance by their workforce.

HIPAA Security Rule

The HIPAA security standards are divided into three categories:

1. **Administrative safeguards:** In general, these are the administrative functions that should be implemented to meet the security standards.
2. **Physical safeguards:** In general, these are the mechanisms required to protect electronic systems, equipment and the data they hold, from threats, environmental hazards and unauthorized intrusion.
3. **Technical safeguards:** In general, these are primarily the automated processes used to protect data and control access to data.

HIPAA Security Rule

Each set of safeguards is comprised of a number of standards which are generally comprised of a number of implementation specifications.

Implementation specifications are either:

- Required: Covered entity must implement policies and/or procedures that meet what the implementation specification requires; or
- Addressable: Covered entity must assess whether it is a reasonable and appropriate safeguard in the entity's environment.
    - *If the covered entity chooses not to implement an addressable specification based on its assessment, it must document the reason and, if reasonable and appropriate, implement an equivalent alternative measure.*

HIPAA Security Rule

Administrative safeguards: Contingency plan - §164.308(a)(7)(i)

- **Standard:** Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure and natural disaster) that damages systems that contain ePHI.

HIPAA Security Rule

Administrative safeguards: Implementation specifications

A. Data backup plan (Required): Establish and implement procedures to create and maintain retrievable exact copies of ePHI.

B. Disaster recovery plan (Required): Establish (and implement as needed) procedures to restore any loss of data.

C. Emergency mode operation plan (Required): Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of ePHI while operating in emergency mode.

HIPAA Security Rule

Administrative safeguards: Implementation specifications

D. Testing and revision procedures (Addressable): Implement procedures for periodic testing and revision of contingency plans.

E. Application and data criticality analysis (Addressable): Assess the relative criticality of specific applications and data in support of other contingency plan components.

HIPAA Security Rule

Physical safeguards: Device and media controls - §164.310(d)(1)

Standard: Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain ePHI into and out of a facility, and the movement of these items within the facility.

Implementation specifications:

(iv) Data backup and storage (Addressable): Create a retrievable exact copy of ePHI, when needed, before movement of equipment.

HIPAA Security Rule

Technical safeguards: Access controls - §164.312(a)(1)

Standard: Implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights.

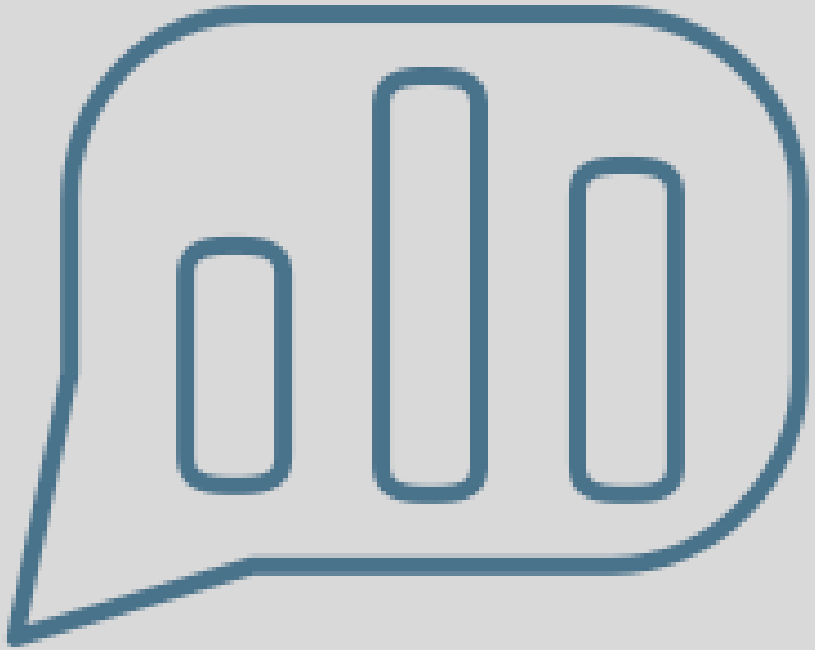
Implementation specifications:

(2)(ii) Emergency access procedure (Required): Establish (and implement as needed) procedures for obtaining necessary ePHI during an emergency

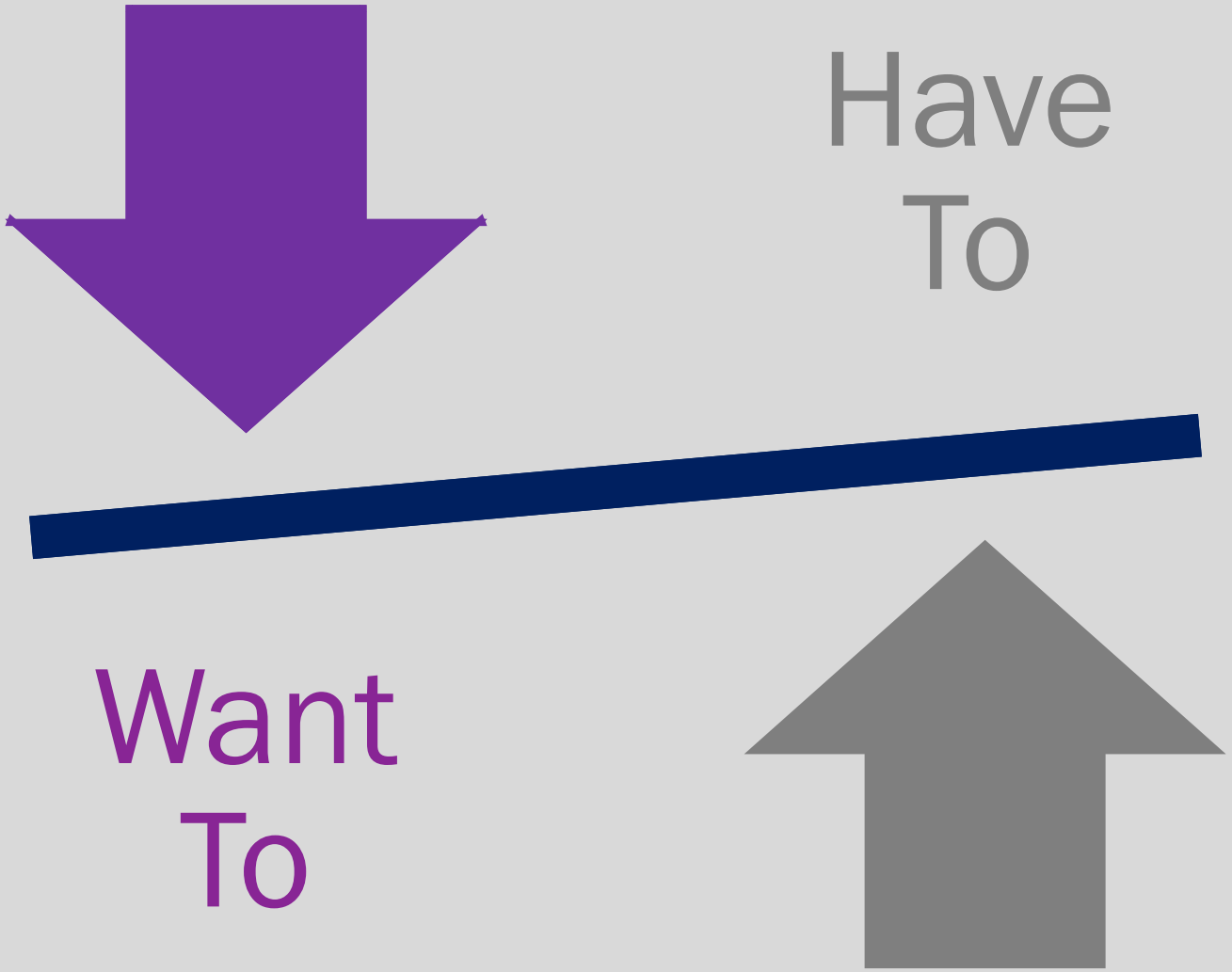
Additional Requirements

- The Joint Commission
- AAAHC (Accreditation Association for Ambulatory Health Care)
- Others

Participant Poll



Why Worry About Cybersecurity?



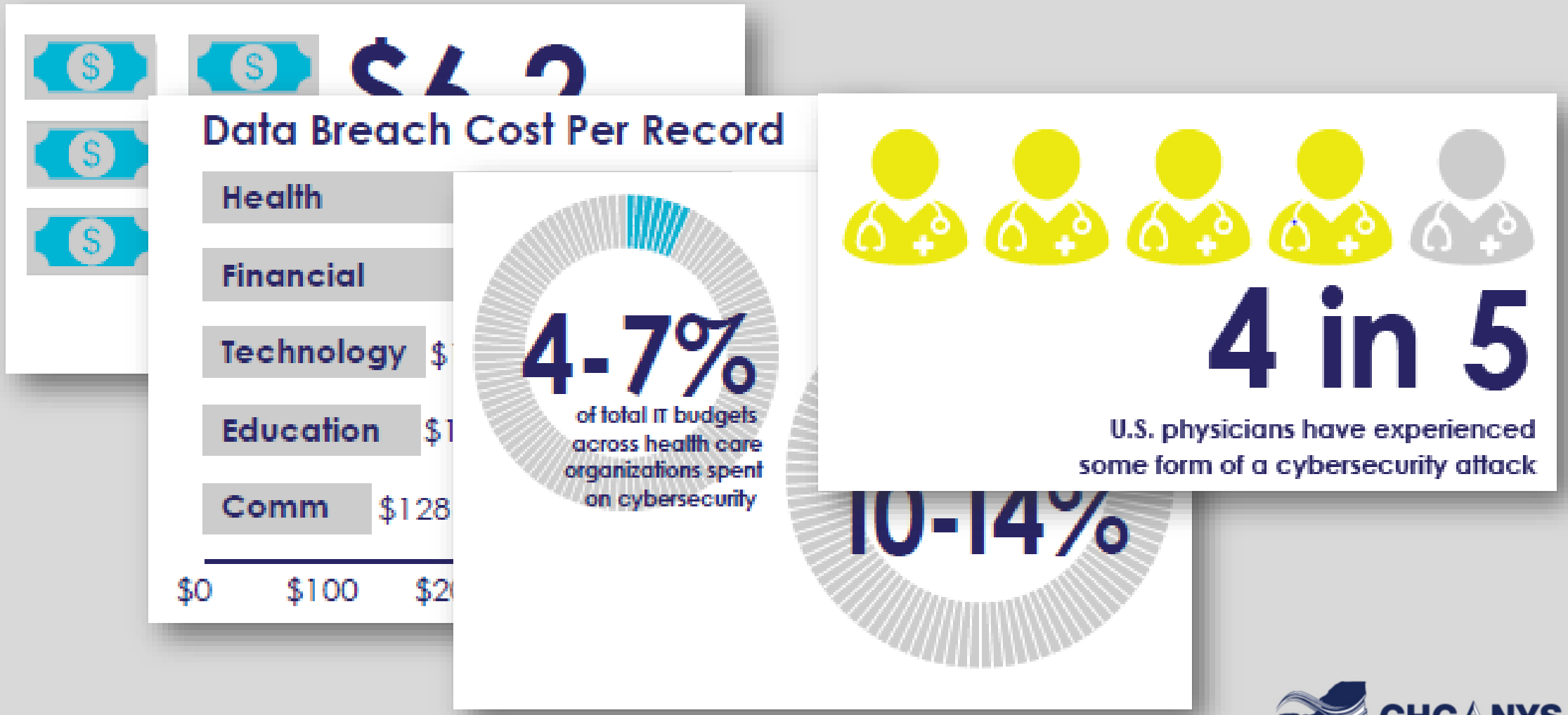
Hackers Love the Health Sector

- Recent U.S. government interagency report indicated average 4,000 daily ransomware attacks on the sector since early 2016;
- 300% increase of ransomware attacks over 2015 - more than any critical infrastructure sector).
  - *Identified 23 different patient safety risks, 55% related to loss of PHI*
- According to TrendMicro, health care was the sector that was hit the hardest by data breaches from 2010 through 2015. Two-thirds were due to the loss or theft of things like laptops, smartphones or thumb drives.
  - *https://www.washingtonpost.com/news/the-switch/wp/2016/03/28/why-hackers-are-going-after-health-care-providers/?noredirect=on&utm_term=.4f1987c5e5ef*

Did You Know?

- Worldwide, the number of cyberattacks increased 40 percent; in 2015, criminal attacks became the number one root cause of data breaches in health care
- Cybercriminals are using cyberattack techniques, tools, tactics and scope that are changing at an exponential pace.
- Cyberattacks using malware or viruses can occur from internal or external sources. Common targets of health care cyberattacks include:
  - *Medical devices (e.g. radiology equipment, blood gas analyzers, therapeutic equipment, and life support equipment)*
  - *Technology equipment, including computers, telephone systems, video conferencing, routers and firewalls*
  - *Clinical EHR software and equipment*
  - *Financial and employee information*
  - *Building control/plant operating systems*
- Health care information is worth 10 times more than credit card numbers on the black market.

Can It Happen to Me?



SOURCE: Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients

Common Vulnerabilities in the Healthcare Sector

- Legacy equipment, technology, software – outdated/no longer supported operating systems; no security patches available;
  - *one legacy system was found to have over 1400 vulnerabilities;*
- Nature of the work: increased need for interconnectivity/internet connected devices
- Rapid roll out without proper secure design or testing
- Lack of workforce training on cyber and network security
- Exploit the human element in a dynamic healthcare environment with frequent staff changes

IT Will Handle It! Right?

IT security professionals are still struggling to fully secure their organizations and protect against breaches, according to a new report:

- Savvier thieves - data is now being stolen by a wide range of methods
- Blame game
- Security technology continues to operate in isolation
- There is a rift in regard to accountability
- Future proofing – IT professionals are purchasing equipment now that could have helped in previous breaches

https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/rp-data-exfiltration-2.pdf

What Would Happen If...

EMERGENCY PREPAREDNESS PROGRAM

Holistic approach to your organizational cybersecurity plans

Emergency Management Defined

Emergency Management –

- An ongoing process to… mitigate, prepare for, respond to, and to recover from, an incident that threatens life, property, operations, or the environment in order to maintain continuity of operations.

Source: National Fire Protection Association, Standard on Disaster/Emergency Management and Business Continuity Programs 1600, p. 5, 2013

EM vs. BCP

Emergency Management (EM)	Business Continuity Planning (BCP)
➢ Focused on the ***response to the specific hazards*** of an emergency or disaster.	➢ Focused on ***maintaining processes to support your organization's essential services*** during an emergency or disaster, as well as those that support restoration of normal operations as quickly as possible.
	➢ Part of the Emergency Operations Plan or maintained separately.

The Emergency Management Cycle

Emergency Management Programs are based on the four phases of the Emergency Management cycle:

Mitigation

Definition - *Sustained action to reduce or eliminate the risks to people and property from hazards and their effects**

- Mitigation actions should be considered long before an event and includes actions designed to reduce the risk to people and property from hazards
  - *Hazard identification and analysis*
  - *Design and construction applications*
  - *Insurance*
  - *Structural Controls*

Mitigation activities take place before and after an event

* *Haddow, G. D., Bullock, J. A., & Coppola, D. P. (2014). Introduction to emergency management. Amsterdam: Elsevier.*

Preparedness

Definition - *A state of readiness to respond to a disaster, crisis, or any other type of emergency situation**

- These are actions and preparations that will improve your chances of successfully dealing with an emergency
  - *Planning*
    - *Developing workforce resiliency*
    - *Continuity of Operations planning*
  - *Training and education*
  - *Exercises*

Preparedness activities take place **before** an event occurs

* *Haddow, G. D., Bullock, J. A., & Coppola, D. P. (2014). Introduction to emergency management. Amsterdam: Elsevier.*

Response

Definition - *Immediate actions to save lives, protect property, and meet basic human needs; responding safely to an event**

- *Response actions are typically keyed to the specific threat*
- *Activation of emergency operations plan and the Emergency Operations Center (EOC)*
- *Response is putting preparedness plans into action*

Response activities take place **during** an event

* *Haddow, G. D., Bullock, J. A., & Coppola, D. P. (2014). Introduction to emergency management. Amsterdam: Elsevier.*

Recovery

Definition – *The development, coordination, and execution of service- and site-restoration plans; operations and services; long-term care and treatment of affected persons; evaluation of the incident to identify lessons learned; post-incident reporting; and development of mitigation initiatives.**

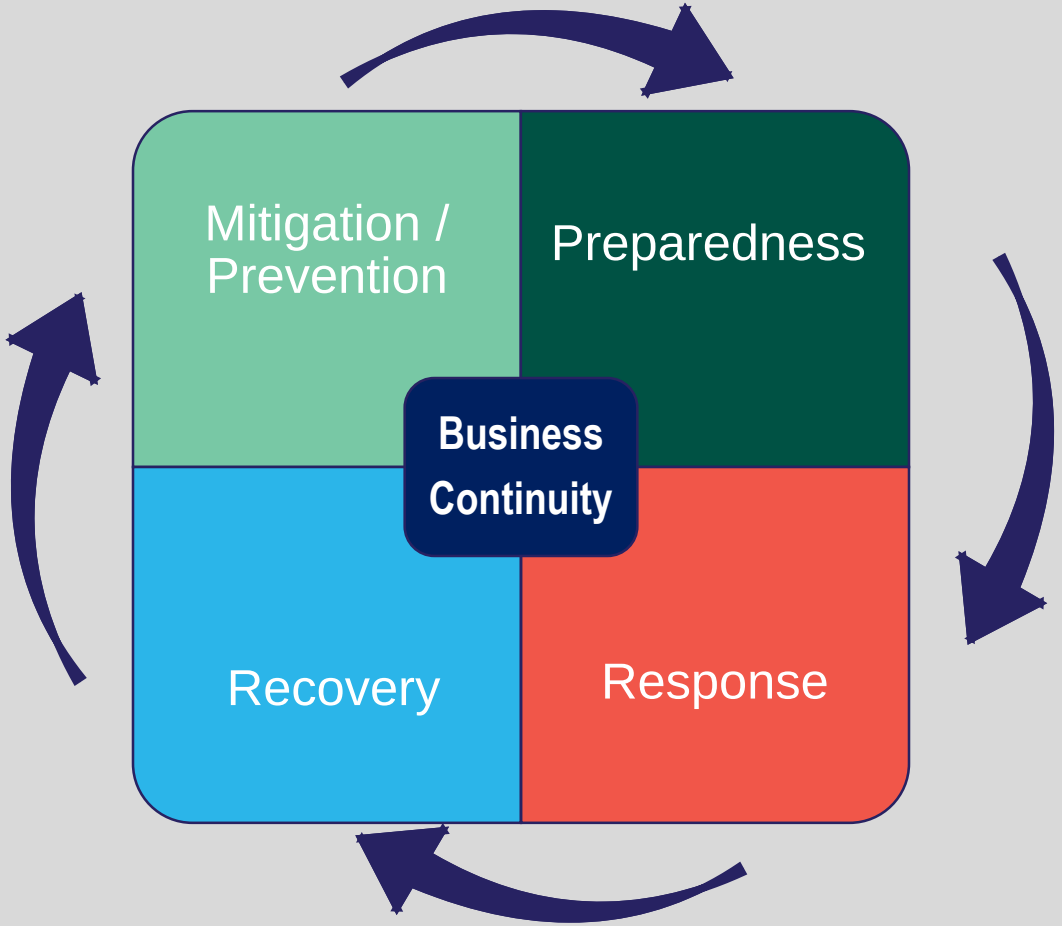
- *Begins as soon as disaster strikes and ends when operations return to "normal"*
- *Short Term vs. Long Term (water main break vs. hurricane);*
- *The development, coordination, and execution of services and site restoration plans;*
- *Evaluation of the incident to identify lessons learned;*
- *Development of initiatives to mitigate the effects of future incidents.*

Recovery activities take place after an event

* *Haddow, G. D., Bullock, J. A., & Coppola, D. P. (2014). Introduction to emergency management. Amsterdam: Elsevier.*

Following Recovery

Following the recovery phase, consider things to do that would lessen or mitigate the effects of future disasters.

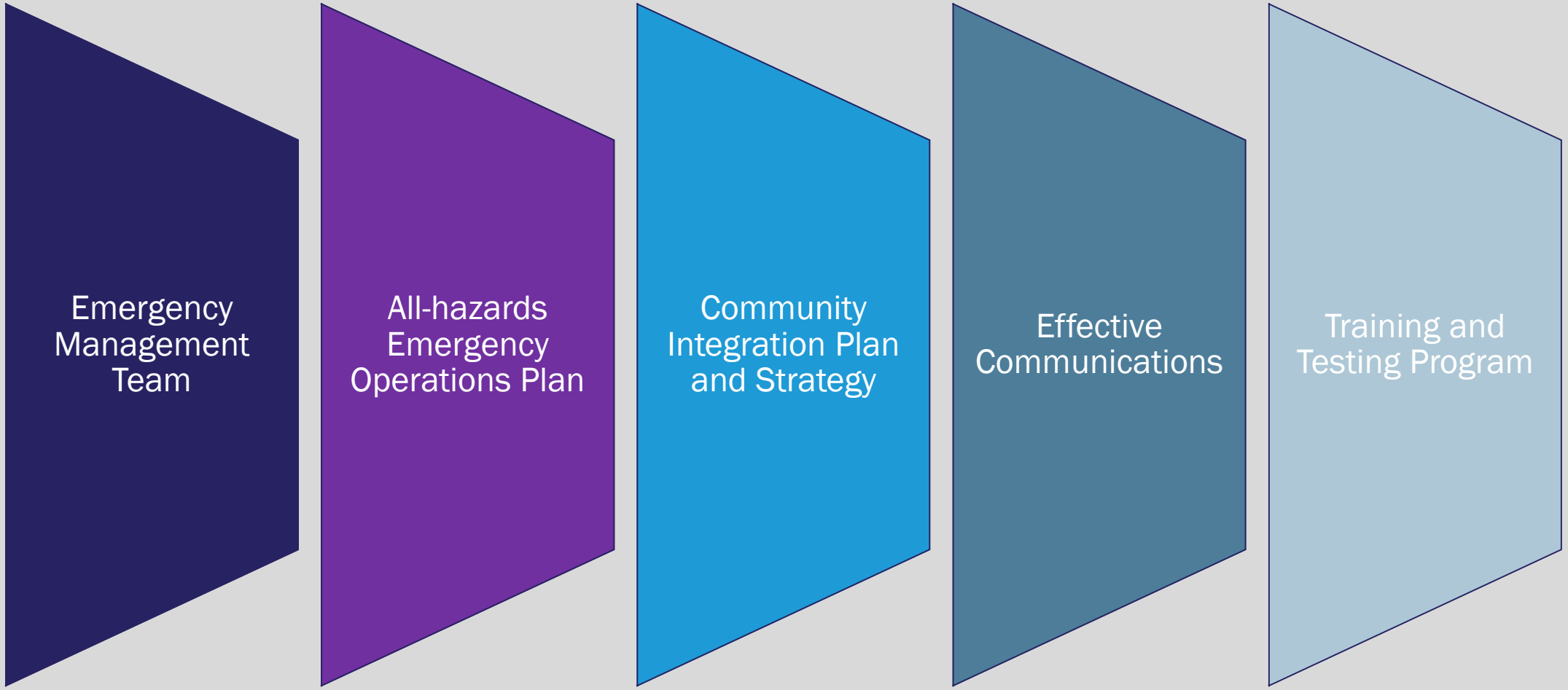


Emergency Management Program Defined

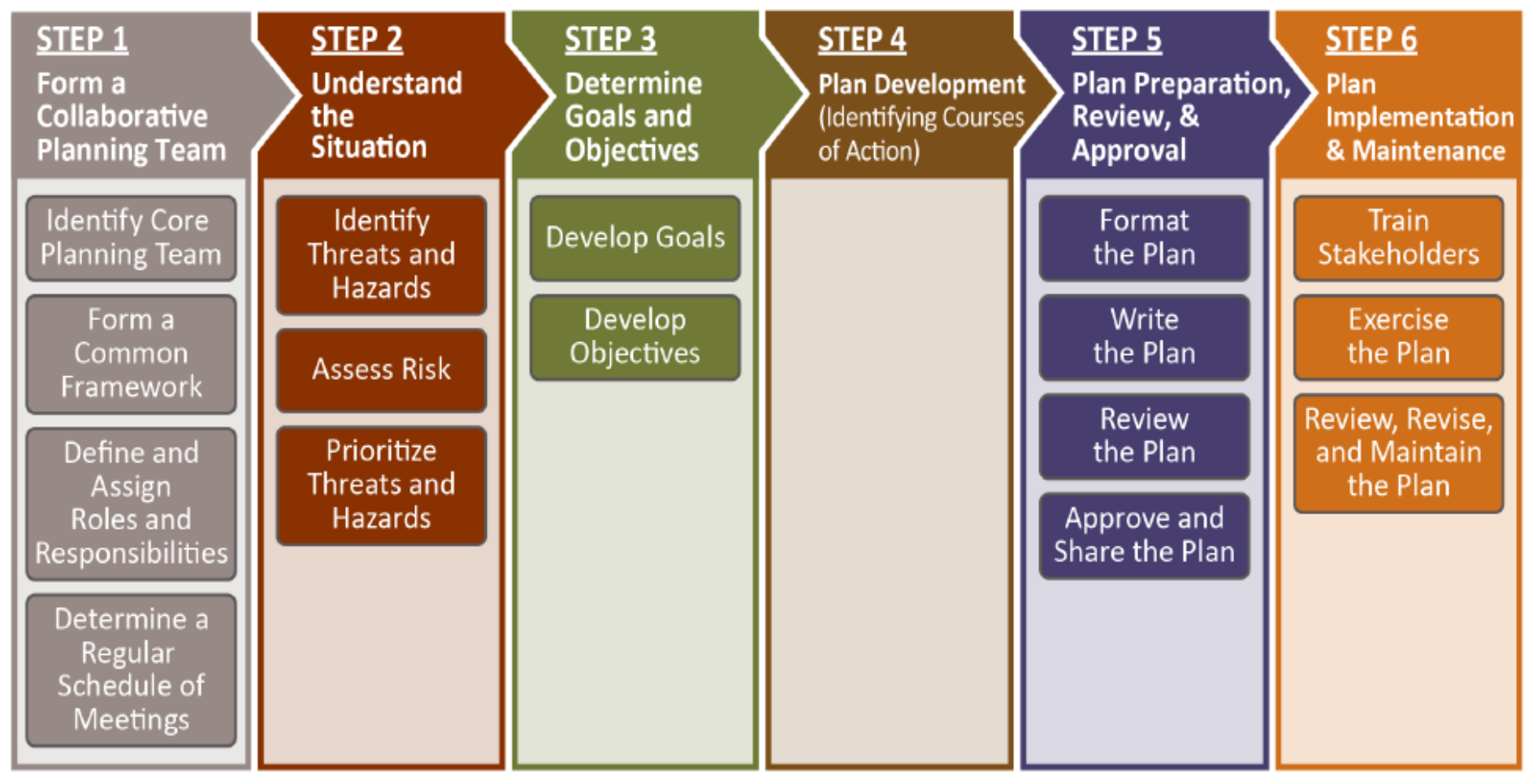
- **Emergency Preparedness Program:**
  - *The Emergency Preparedness Program describes a facility's **comprehensive** approach to meeting the health, safety and security needs of the facility, its staff, their patient population and community prior to, during and after an emergency and disaster.*

Source: CMS EP Rule Interpretive Guidelines

EM Program Essential Components



Steps in the EM Planning Process



Source: FEMA

https://www.fema.gov/media-library/assets/documents/25975

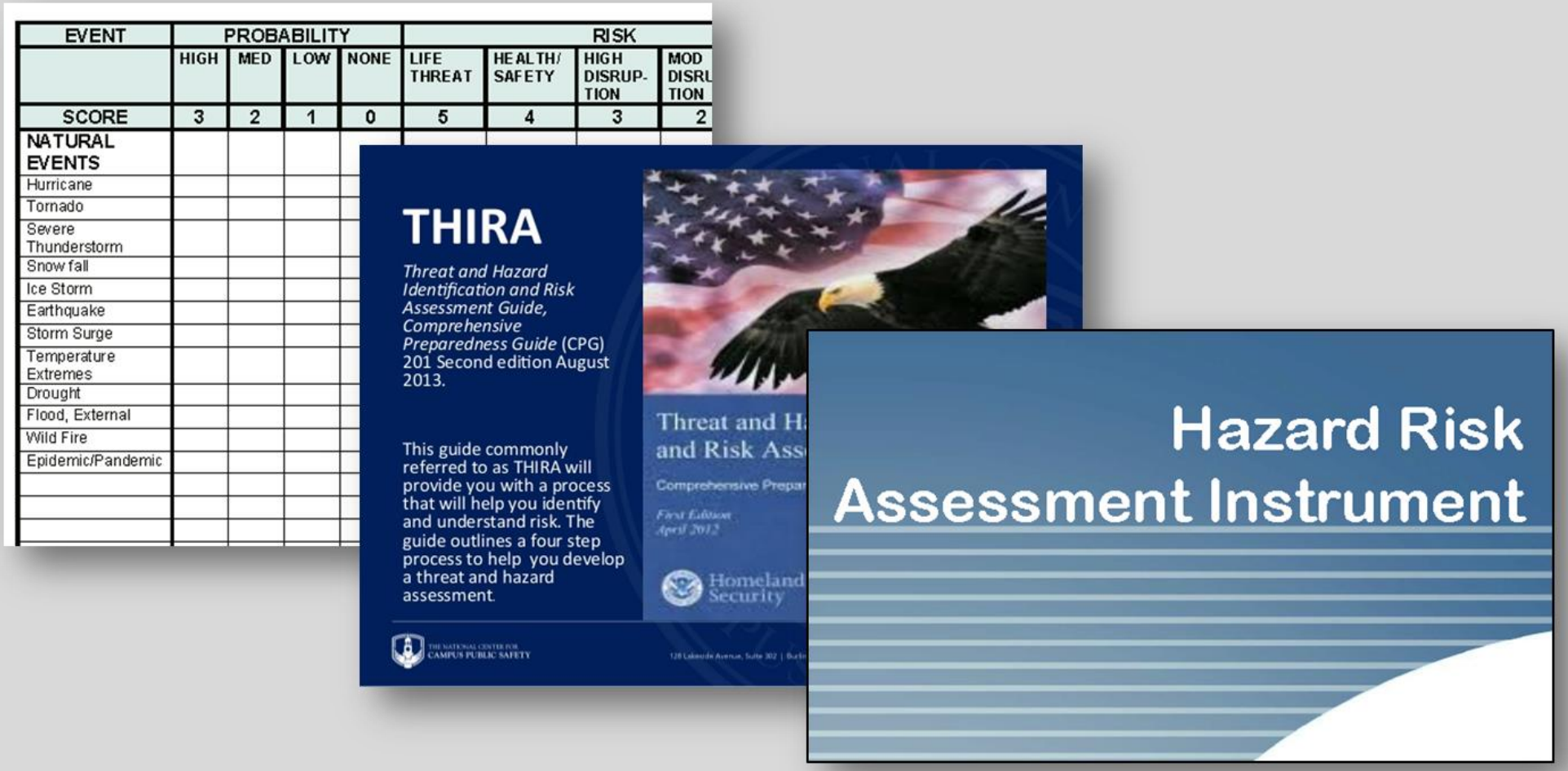
RISK ASSESSMENT

HVA/Risk Assessment Defined

Hazard vulnerability analysis (HVA) and **risk assessment** are systematic approaches to identifying hazards or risks that are most likely to have an impact on a healthcare facility and the surrounding community.

https://asprtracie.hhs.gov/technical-resources/3/hazard-vulnerability-risk-assessment/1

Examples of Risk Assessment/HVA Tools



HVA Terms

Risk Assessment / Emergency Planning

- **Probability** - Likelihood this will occur
- **Severity = (Magnitude - Mitigation)**
  - ***Magnitude*** *- Human, Property, and/or Business Impact*
  - ***Mitigation*** *- Preparedness and Internal/External Response Capabilities*

Priority Planning

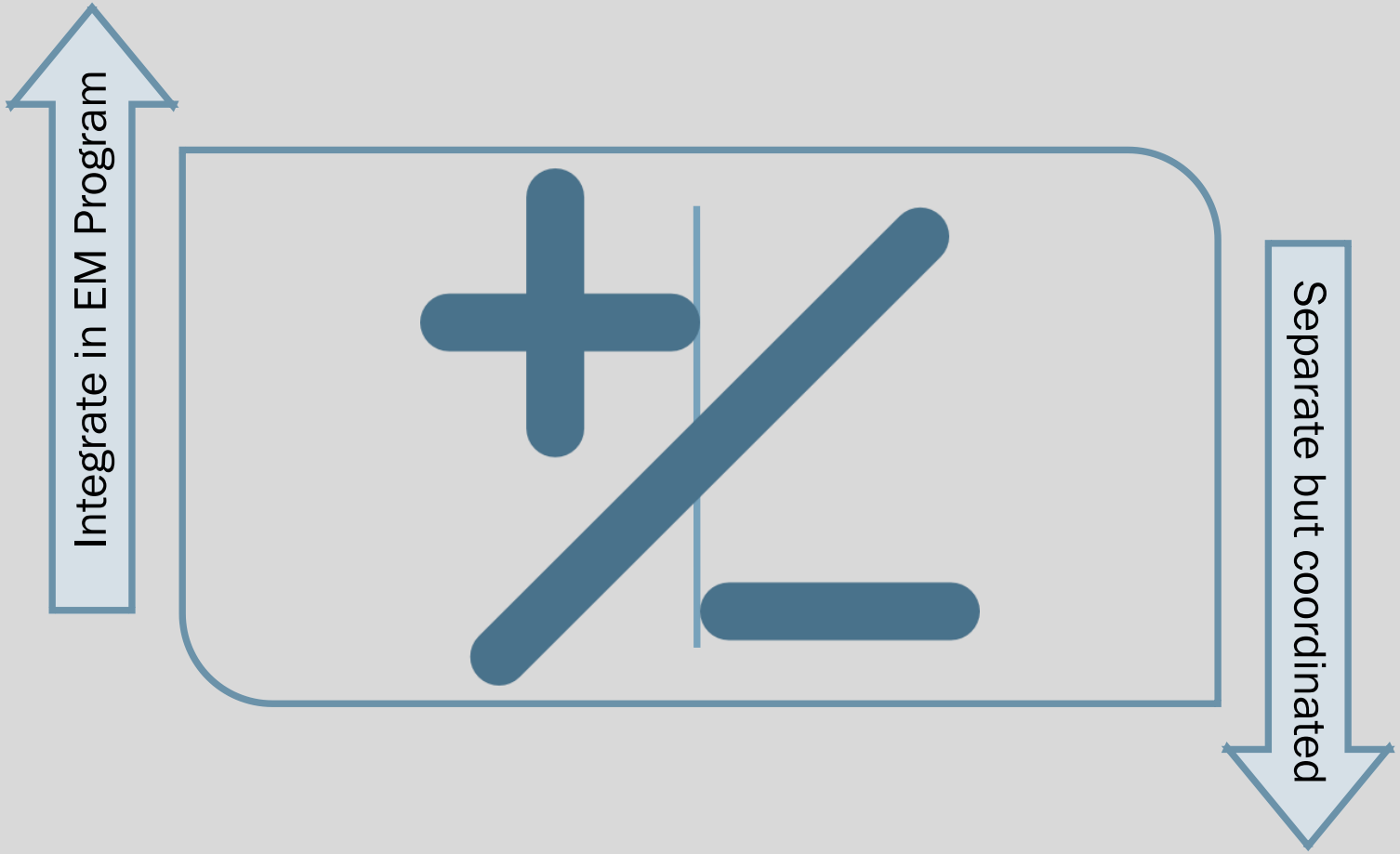
- Based on the top risks identified by the HVA for each health center location, the health center should establish hazard specific plans.

EXAMPLE: XYZ FQHC's top 5 priorities

1. *Inclement Weather*
2. *Coastal Storm*
3. *Active Shooter Threat*
4. *Cybersecurity Attack*
5. *Infectious Disease Outbreak*

CREATING AN APPROPRIATE PLAN

Integrate or Separate?



Emergency Operations Plan (EOP)

- **Emergency Management Plan:**
  - *A <u>continually</u> updated document describing the comprehensive system of principles, policies, procedures, methods, and activities to be applied in response to a variety of emergencies and disasters.*

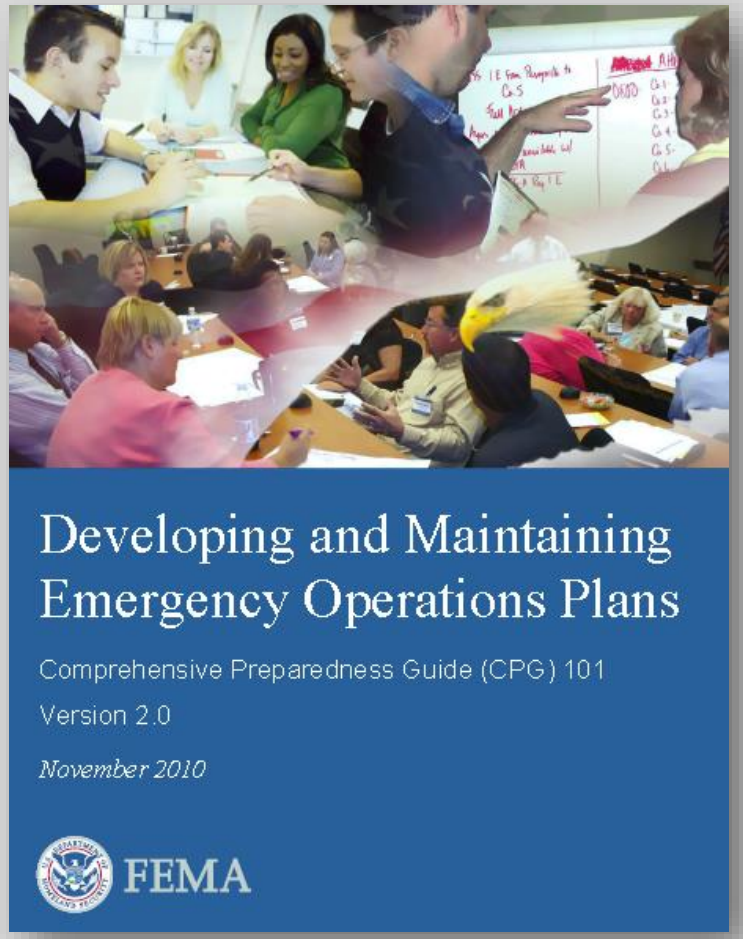
Source: HRSA Bureau of Primary Health Care Policy Information Notice 2007-15

- **Emergency Plan:**
  - *An Emergency Plan provides the framework for the emergency preparedness program. The emergency plan is developed based on facility- and community-based risk assessments that assist a facility in anticipating and addressing facility, patient, staff and community needs and support continuity of business operations.*

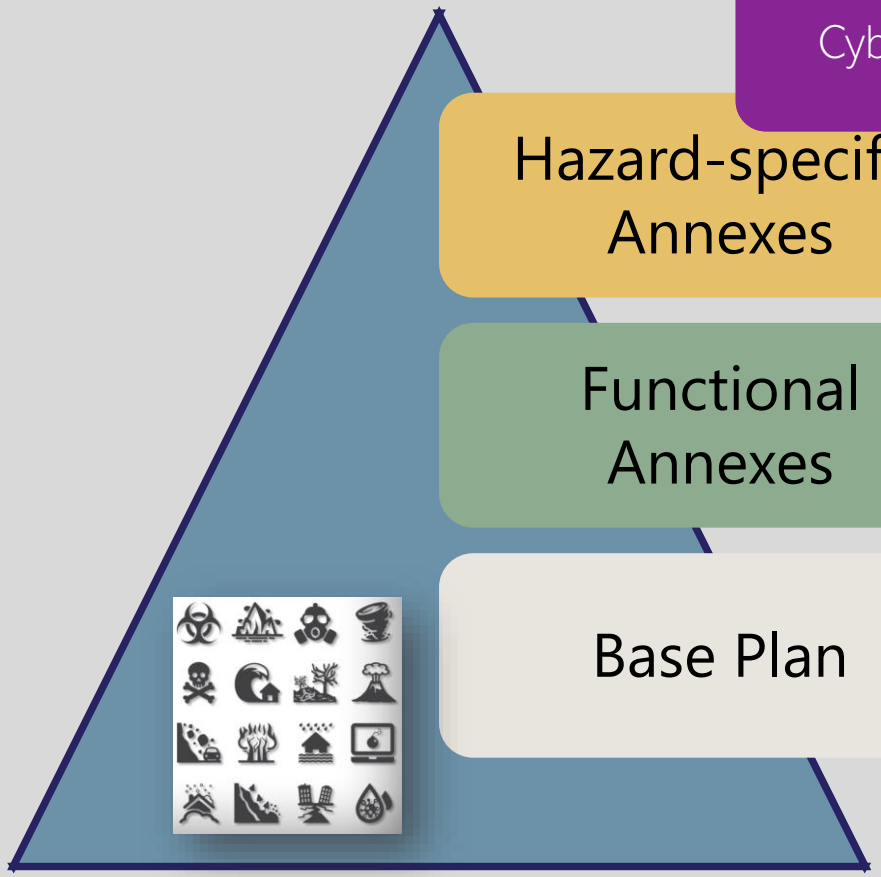
Source: CMS EP Rule Interpretive Guidelines

EOP Traditional Format

- **Base Plan**
  - *Intro, Purpose, Communications, Finance etc.*
- **Functional Annexes**
  - *Business Continuity, Volunteer Management, Evacuation, Fire Safety, etc.*
- **Hazard-, Threat-, or Incident- Specific Annexes**
  - *Coastal Storm, Infectious Disease, Cyberattack, Inclement Weather, Active Shooter, etc.*



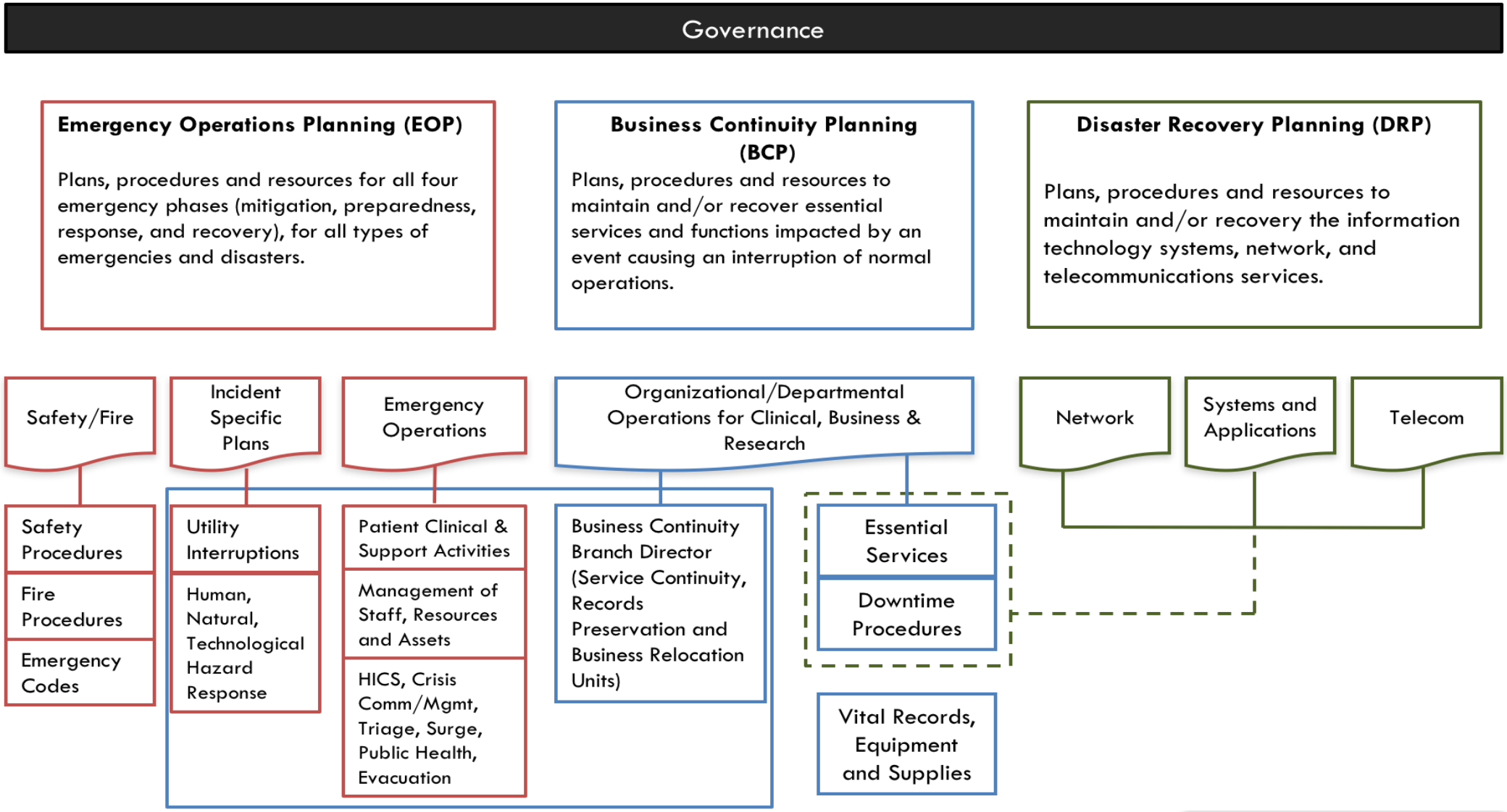
Traditional Format



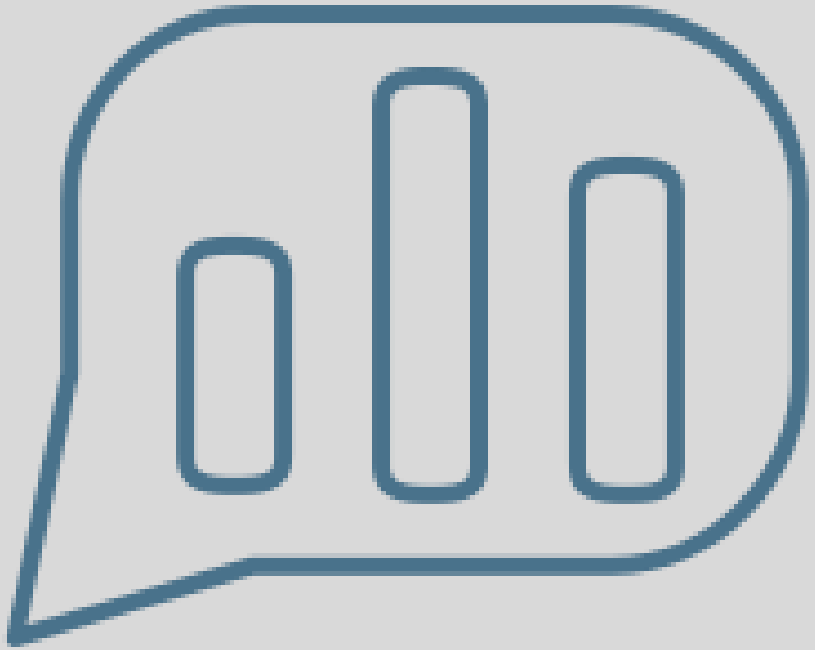
- Cybersecurity
- Inclement Weather
- Coastal Storm
- Active Shooter Threat
- Infectious Disease Outbreak

Healthcare Emergency Management & Business Continuity Framework

Continuity I Response I Recovery



Participant Poll



Emergency Operations Plan

- *Available for download*
- *https://www.nurseledcare.org/documents/item/567-health-center-emergency-management-plan-preview.html*

Proposed Health Center Plan Elements

- ✓ Introduction
  - *Authorization, revisions, distribution*
1. Program Administration
   - *Summary, Purpose, Scope, EMC*
2. Situation and Assumptions
   - *HVA, key assumptions*
3. Command and Control
   - *ICS, authority, (de)activation, roles & responsibilities*
4. Continuity of Operations
   - *Essential functions*
5. Communications
   - *Risk communications, notifications, partners*
6. Buildings, Utilities, Safety and Security
   - *Facilities, evacuation, utility, safety & security*
7. Finance, Logistics and Staff Care
   - *EOC, supplies, volunteers, staff scheduling and care, HR, payroll*
8. Community Integration
   - *Partners, coalitions, agreements, MH*
9. Plan Development and Maintenance
   - *Development, review, storage, training, testing*
10. Hazard Specific Plans
11. Standards, Regulations and Guidelines

Plan Elements

INTRODUCTION

- Title page and table of contents
- Authorization or what makes the plan “official”
- Revision record, i.e. what, when and who revised
- Distribution record, i.e. when, how and who received it

Plan Elements

SECTION 1 - Program Administration

- Provides an executive summary of the plan
- Describes plan's objectives and scope
- Designates an Emergency Management Committee

Plan Elements

SECTION 2 - Situation and Assumptions

- Describes health center's Hazard Vulnerability Analysis (HVA) process, identifies potential hazards and risks to the health center and identifies top planning priorities.
- Outlines key assumptions of the plan, e.g. Health Center will experience top hazards as well as other lesser hazards; Health Center is required and expected to conduct emergency preparedness activities etc.

Plan Elements

SECTION 3 - Command and Control

- Outlines Health Center's Incident Command System (ICS), roles and organizational chart
- Outlines procedures for the activation and deactivation of the Plan
- Describes procedures for incident action planning and information collection, documentation, dissemination
- Specifies roles of the health center and other partners across four phases of emergency management

Plan Elements

SECTION 4 – Continuity of Operations

- Identifies health center's essential functions (i.e. those that must continue during an emergency / disaster) and supporting processes.
- Refers to a more detailed Business Continuity Plan (BCP) and additional relevant information, such as insurance.

Plan Elements

SECTION 5 - Communications

- Describes policies and protocols for communication with the health center's staff, patients, the community, local partners, and response agencies
- Outlines procedures for risk communications and public information
- Identifies primary and alternate communications systems
- Identifies procedures for communication exercises

OR refers to a more detailed Communications Plan and additional relevant information, such as contact information details.

Definition of an Emergency Preparedness Communication Plan

An emergency preparedness communications plan is a document that provides guidelines, contact information and procedures for how information should be shared during all phases of an unexpected occurrence that requires immediate action.

Communication Plan

This document describes the following:

1. The procedure to notify staff that emergency response has been initiated.
2. The steps the facility will use to communicate information and instructions to its staff during an emergency.
3. The procedures to notify external authorities that emergency response measures have been initiated and communicate during the emergency.
4. How the facility will communicate with patients and their families.
5. How the facility will communicate with the community or the media during an emergency, including designation of a Public Information Officer (PIO)
6. How the facility will communicate with suppliers of essential services, equipment, and supplies during an emergency.

Communication Plan (cont.)

7. How the facility will communicate with other health care organizations in its geographic area regarding the essential elements of their respective command structures, the resources and assets that could be shared in an emergency response.
8. How the organization will communicate and under what circumstances will the organization communicate the names of patients and the deceased with other health care organizations in its geographic area.
9. How the organization will communicate and under what circumstances will the organization communicate information about patients to third parties.
10. What primary and alternate communication methods the organization will use.
11. How the organization will do maintenance / testing of data, equipment/software, and protocols.

Communications Plan

Available for download:

- https://www.nurseledcare.org/documents/item/568-health-center-communications-plan-preview.html

Plan Elements

SECTION 6 – Buildings, Utilities, Safety and Security

- Describes management of facilities (e.g. considerations for space owned vs. leased, regular inspections etc.)
- Refers to detailed evacuation, sheltering in place, fire safety, utility disruption, safety & security plans / policies
- Identifies responsible staff titles

Plan Elements

SECTION 7 - Finance, Logistics and Staff Care

- Identifies Emergency Operations Center (EOC) or Command Center for the health center
- Describes plans to maintain the health center's supply chain (e.g., delivery of Personal Protective Equipment, vaccines)
- Identifies policies for volunteer management
- Provides direction on relevant human resource policies, staff schedules, expense tracking etc.

Plan Elements

SECTION 8 - Community Integration

- Identifies health center's key partners and how the center's plans are integrated into the systems framework of planning
- Plans for the integration of health center's services into the community-wide response plans
- Lists standing agreements with partners, coalitions, responders, and other agencies
- Addresses emergency mental health provision policies

Plan Elements

SECTION 9 – Plan Development and Maintenance

- Describes how the Plan is developed, maintained, approved, distributed and stored
- Describes health center's training program
- Includes policies and procedures for the evaluation of training and exercises
- Describes methods to integrate lessons learned from both exercises and actual events into the plan and primary care center operations

Plan Elements

SECTION 10 - Hazard Specific Plans

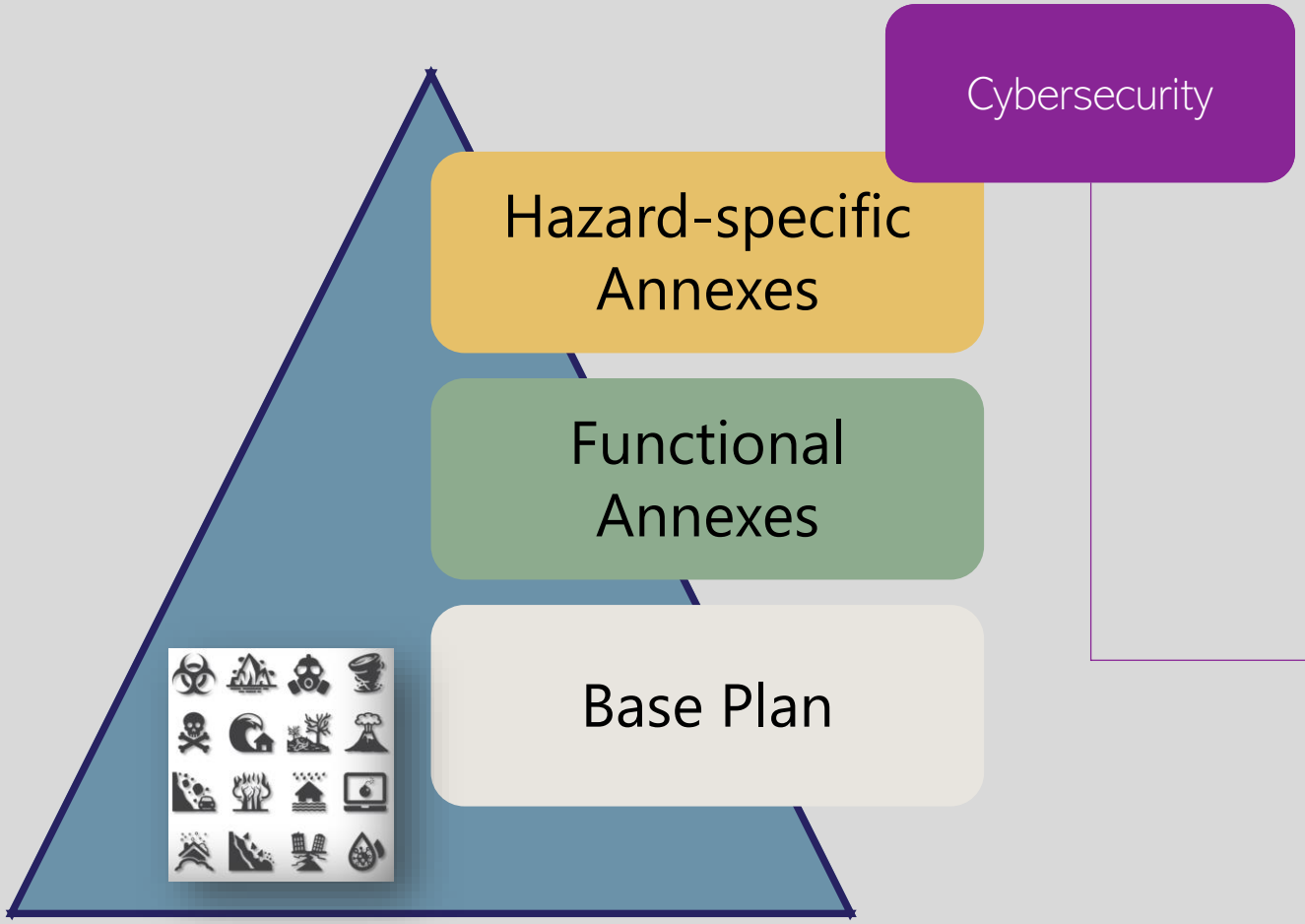
- Briefly describes hazard-specific plans / protocols for the organization and refers to the detailed plans attached as **Annexes**, which:
  - Include plans that address specific hazards identified in the HVA, such as coastal storms and pandemics
  - Include the four phases of emergency management (mitigation, preparedness, response, and recovery) in each plan
  - Build upon the other elements of the Emergency Management Plan
  - Include information about the specific hazard and response and recovery needs of the health center

Plan Elements

SECTION 11 – Standards, Regulations and Guidelines

- Lists all relevant regulatory standards that are applicable for the Plan and the health center (e.g. CMS EP Final Rule, HRSA PIN 2007-15, state regulations, etc.)

Bringing It All Together



Coming Up Next!

February 26

Part II – Cybersecurity Hazards: Threat, Assessment & Recovery

- *Focus on cybersecurity as a specific hazard, assessment of vulnerabilities, making a robust plan and recovering quickly when affected.*

REGISTER HERE

Webinar Evaluation

We value your feedback!

Questions?

NYS HCCN

hccn@chcanys.org