CHCANYS NYS-HCCN

# Using Emergency Management for Cybersecurity Preparedness, Response, and Recovery

## WORKSHOP

Anne Hasselmann, MPH
*ARH Health Consulting, LLC*

Alexander Lipovtsev, LCSW
*CHCANYS*

# 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*

# Objectives

1. Define the importance of including staff responsible for maintaining security for your organization's Information Technology/Information Systems (IT/IS) in emergency management (EM) and business continuity (BC) planning.
2. Discuss how response and recovery for a cybersecurity incident may be managed through the Incident Command Structure (ICS).
3. Describe how emergency management, business continuity, and disaster recovery complement each other and apply this knowledge to incident action planning for IT/IS loss due to a security incident.

# Why Should Health Centers Care About Cybersecurity?

- Health care information is worth 10 times more than credit card numbers on the black market.

# 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

# Cyberattacks Can Occur From Internal or External Sources

- Cyberattack techniques, tools, tactics and scope are changing at an exponential pace.
- Common targets of health care cyberattacks from malware or viruses 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.

# Cybersecurity and Health Centers: The Rules

# CMS Emergency Preparedness Rule

- CMS issued Emergency Preparedness Requirements for Medicare and Medicaid Participating Providers and Suppliers to:
  - 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.
- Initial rule became effective November 15, 2016.
- Revisions became effective November 29, 2019.

Medicare and Medicaid Programs; Emergency Preparedness Requirements for Medicare and Medicaid Participating Providers and Suppliers" Final Rule (81 FR 63860, Sept. 16, 2016).

Medicare and Medicaid Programs; Regulatory Provisions To Promote Program Efficiency, Transparency, and Burden Reduction; Fire Safety Requirements for Certain Dialysis Facilities; Hospital and Critical Access Hospital (CAH) Changes To Promote Innovation, Flexibility, and Improvement in Patient Care Final Rule (84 FR 51732, Sept. 30, 2019).

# CMS EP Rule: Provisions Intended to Maintain Access to Health Care Services During Emergencies

- Focused on 3 essential elements to maintain access to care:
  - Safeguarding human resources.
  - Maintaining business continuity.
  - Protecting physical resources.
- Participating providers must have:
  - An “All-Hazards” comprehensive emergency management program (CEMP) and plan (including policies and procedures to support execution of the plan).
  - Communications Plan.
  - Training and Testing program that includes initial emergency preparedness training for new and existing staff and annual refresher trainings.

*Appendix Z- EP SOM February 2019

# All-Hazards Approach to Emergency Preparedness

- Integrated approach that focuses on developing capacities and capabilities to address 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.

# NYS Title 10 - Section 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

# Health Center Program Compliance Manual

*Health Center Program Compliance Manual*

**Appendix A: Health Center Program Non-Regulatory Policy Issuances That Remain in Effect**

The following policy issuances most often referred to as Policy Information Notices (PINs) remain in effect and are not superseded by the Health Center Program Compliance Manual:

PIN 2007-09 Service Area Overlap: Policy and Process (http://bphc.hrsa.gov/programrequirements/policies/pin200709.html)

PIN 2007-15 Health Center Emergency Management Program Expectations (https://bphc.hrsa.gov/about/pdf/pin200715.pdf)

PIN 2008-01 Defining Scope of Project and Policy for Requesting Changes (http://bphc.hrsa.gov/programrequirements/policies/pin200801.html)

PIN 2009-02 Specialty Services and Health Centers' Scope of Project (http://bphc.hrsa.gov/programrequirements/policies/pin200902purpose.html)

PIN 2009-05 Policy for Special Population-Only Grantees Requesting a Change in Scope to Add a New Target Population (http://bphc.hrsa.gov/programrequirements/policies/pin200905specialpops.html)

The following HRSA/BPHC policy documents and resources also remain in effect and are not superseded by the Health Center Program Compliance Manual:

Federal Tort Claims Act Health Center Policy Manual (https://bphc.hrsa.gov/ftca/pdf/ftcahcpolicymanualpdf.pdf)

Additional Scope of Project/Change in Scope Resources (http://bphc.hrsa.gov/programrequirements/scope.html)

Site Visit Resources (http://bphc.hrsa.gov/programrequirements/svguide.html)

Uniform Data System (UDS) Resources (http://bphc.hrsa.gov/datareporting/reporting/index.html)

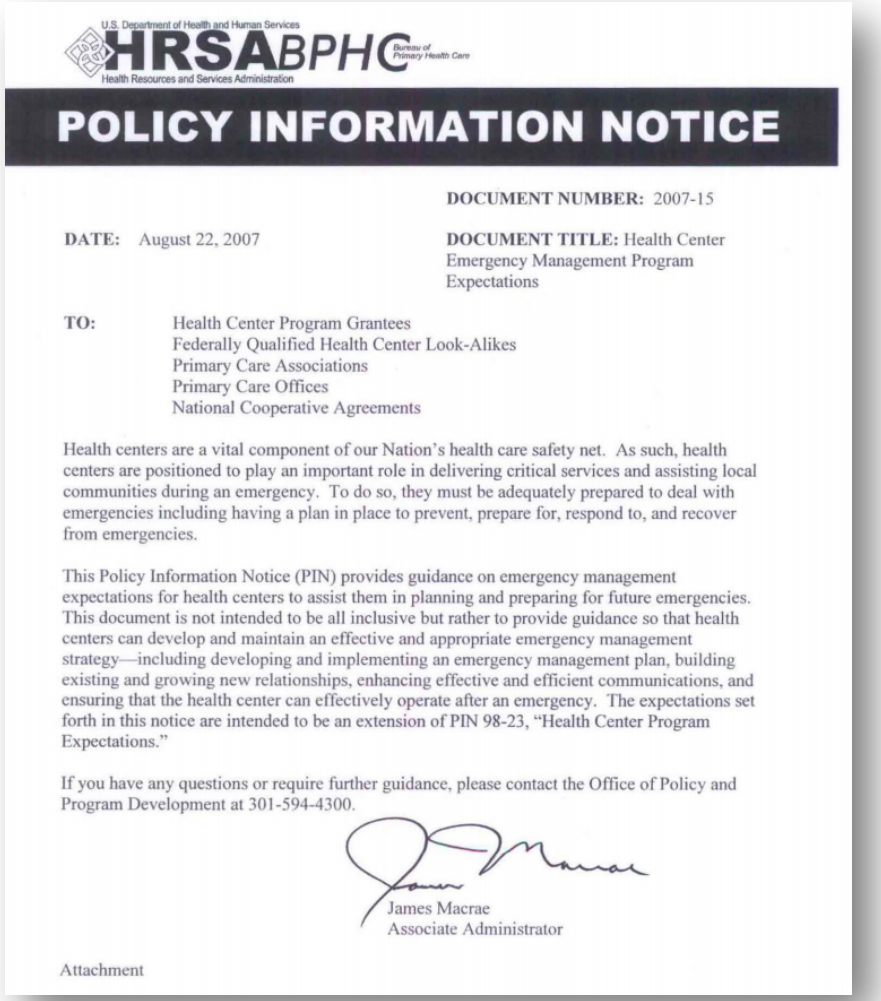
- The following policy issuances most often referred to as Policy Information Notices (PINs) remain in effect and are not superseded by the Health Center Program Compliance Manual:
- […]
- PIN 2007-15 Health Center Emergency Management Program Expectations (https://bphc.hrsa.gov/about/pdf/pin200715.pdf)

https://bphc.hrsa.gov/programrequirements/compliancemanual/appendix.html



CHCANYS

# PIN 2007-15 "Health Center Emergency Management Program Expectations"



U.S. Department of Health and Human Services
HRSA BPHC Bureau of Primary Health Care
Health Resources and Services Administration

**POLICY INFORMATION NOTICE**

**DOCUMENT NUMBER:** 2007-15

**DATE:** August 22, 2007

**DOCUMENT TITLE:** Health Center Emergency Management Program Expectations

**TO:** Health Center Program Grantees
Federally Qualified Health Center Look-Alikes
Primary Care Associations
Primary Care Offices
National Cooperative Agreements

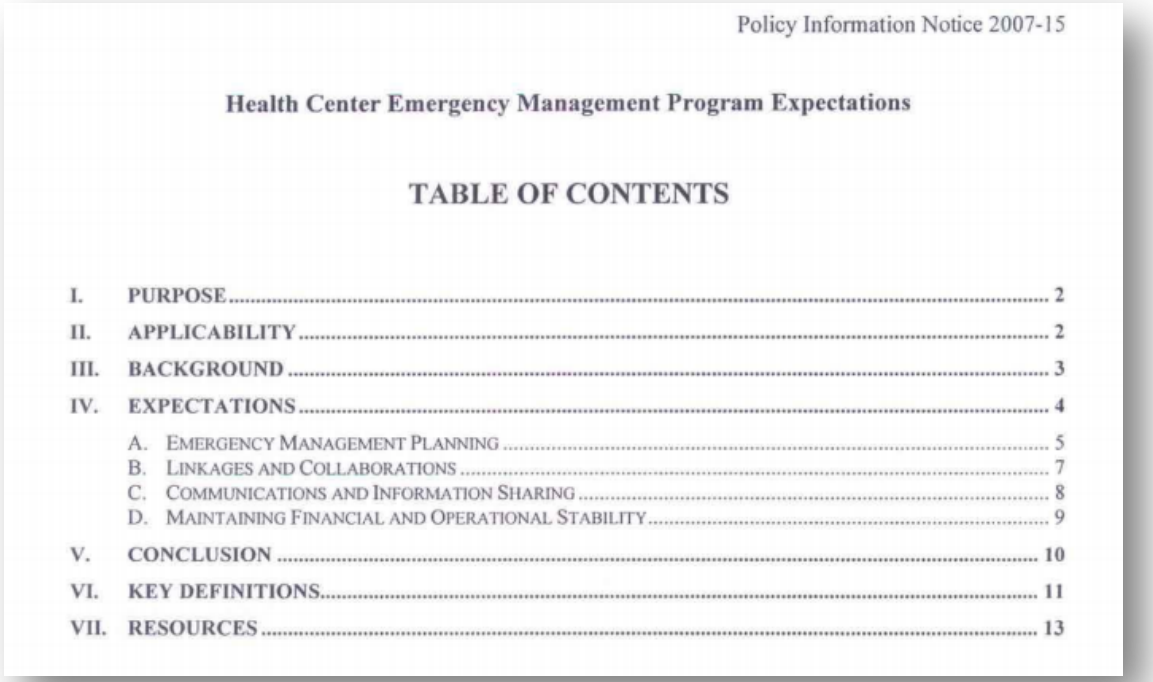
Health centers are a vital component of our Nation's health care safety net. As such, health centers are positioned to play an important role in delivering critical services and assisting local communities during an emergency. To do so, they must be adequately prepared to deal with emergencies including having a plan in place to prevent, prepare for, respond to, and recover from emergencies.

This Policy Information Notice (PIN) provides guidance on emergency management expectations for health centers to assist them in planning and preparing for future emergencies. This document is not intended to be all inclusive but rather to provide guidance so that health centers can develop and maintain an effective and appropriate emergency management strategy—including developing and implementing an emergency management plan, building existing and growing new relationships, enhancing effective and efficient communications, and ensuring that the health center can effectively operate after an emergency. The expectations set forth in this notice are intended to be an extension of PIN 98-23, "Health Center Program Expectations."

If you have any questions or require further guidance, please contact the Office of Policy and Program Development at 301-594-4300.

James Macrae
Associate Administrator

Attachment



Policy Information Notice 2007-15

**Health Center Emergency Management Program Expectations**

**TABLE OF CONTENTS**





CHCANYS

# Additional PINs/PALs of Relevance

- Request a Change in Scope of Project to Add a Temporary Site(s): PAL 2020-05. Contact your project officer with health center grant or scope of project questions.
- PAL 2020-01 - Telehealth and Health Center Scope of Project
- Federal Tort Claims Act (FTCA) Resources:
  - FTCA Coverage When Responding to Emergency Events
  - Temporary Privileging of Clinical Providers in Emergency Situations - PAL 2017-07
  - Health Center Volunteer Health Professional Deeming Application Instructions

# HRSA Form 10: Emergency Preparedness Report – NAP Application

**Form 10: Emergency Preparedness Report**

OMB No.: 0915-0285. Expiration Date: 1/31/2020

| DEPARTMENT OF HEALTH AND HUMAN SERVICES<br>Health Resources and Services Administration<br><br>Form 10: EMERGENCY PREPAREDNESS REPORT | FOR HRSA USE ONLY<br>Grant Number | <br>Application Tracking Number |
|---|---|---|
| | | |

| Section I: Emergency Preparedness and Management (EPM) Plan | |
|---|---|
| 1. Has your organization conducted a thorough Hazards Vulnerability Assessment?<br>If Yes, date completed:_____ | ☐ Yes ☐ No |
| 2. Does your organization have an approved EPM plan?<br>If Yes, date that the most recent EPM plan was approved by your Board:_____<br>If No, skip to the Readiness section below. | ☐ Yes ☐ No |
| 3. Does the EPM plan specifically address the four disaster phases?<br>(This question is mandatory if you answered Yes to question 2.) | ☐ Yes ☐ No |
| 3a. Mitigation | ☐ Yes ☐ No |
| 3b. Preparedness | ☐ Yes ☐ No |
| 3c. Response | ☐ Yes ☐ No |
| 3d. Recovery | ☐ Yes ☐ No |
| 4. Is your EPM plan integrated into your local/regional emergency plan?<br>(This question is mandatory if you answered Yes to question 2.) | ☐ Yes ☐ No |
| 5. If No, has your organization attempted to participate with local/regional emergency planners?<br>(This question is mandatory if you answered Yes to question 2 and No to question 4.) | ☐ Yes ☐ No |
| 6. Does the EPM plan address your capacity to render mass immunization/prophylaxis?<br>(This question is mandatory if you answered Yes to question 2.) | ☐ Yes ☐ No |
| **Section II: READINESS** | |
| 1. Does your organization include alternatives for providing primary care to the current patient population if you are unable to do so during an emergency? | ☐ Yes ☐ No |
| 2. Does your organization conduct annual planned drills? | ☐ Yes ☐ No |
| 3. Does your organization's staff receive periodic training on disaster preparedness? | ☐ Yes ☐ No |
| 4. Will your organization be required to deploy staff to Non-Health Center | ☐ Yes ☐ No |

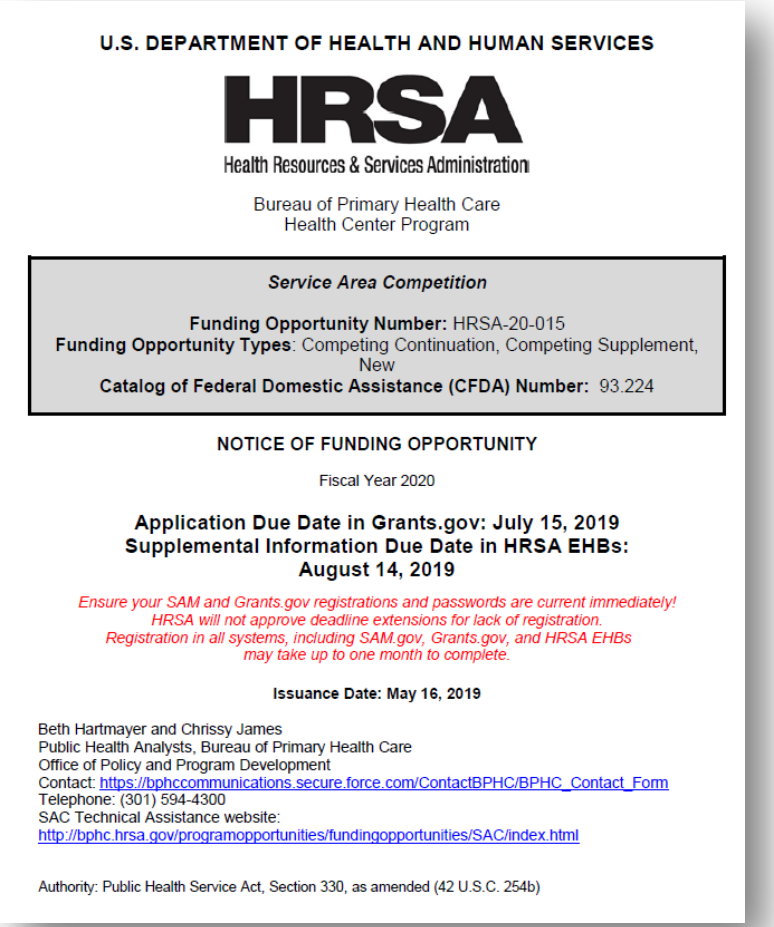
- Required for *New Access Point (NAP)* application submission

**Form 10: Emergency Preparedness Report**

Select the appropriate responses regarding emergency preparedness.

# Service Area Competition (SAC)

- A question on **maintaining continuity of services during disasters and emergencies** in the Project Narrative: RESOURCES/CAPABILITIES section replaced *Form 10: Emergency Preparedness.*
- **RESOURCES/CAPABILITIES** – Corresponds to Section V.1 Review Criterion 5: RESOURCES/CAPABILITIES
  - 7) Describe your current capability and/or plans for maintaining continuity of services and responding to urgent primary health care needs during disasters and emergencies*, including:
    a) Response and recovery plans.
    b) Backup systems to facilitate communications.
    c) Patient records access.
    d) Integration into state and local preparedness plans.



U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES

HRSA
Health Resources & Services Administration

Bureau of Primary Health Care
Health Center Program

*Service Area Competition*

**Funding Opportunity Number:** HRSA-20-015
**Funding Opportunity Types**: Competing Continuation, Competing Supplement, New
**Catalog of Federal Domestic Assistance (CFDA) Number:** 93.224

**NOTICE OF FUNDING OPPORTUNITY**

Fiscal Year 2020

**Application Due Date in Grants.gov: July 15, 2019**
**Supplemental Information Due Date in HRSA EHBs: August 14, 2019**

*Ensure your SAM and Grants.gov registrations and passwords are current immediately! HRSA will not approve deadline extensions for lack of registration. Registration in all systems, including SAM.gov, Grants.gov, and HRSA EHBs may take up to one month to complete.*

**Issuance Date: May 16, 2019**

Beth Hartmayer and Chrissy James
Public Health Analysts, Bureau of Primary Health Care
Office of Policy and Program Development
Contact: https://bphccommunications.secure.force.com/ContactBPHC/BPHC_Contact_Form
Telephone: (301) 594-4300
SAC Technical Assistance website:
http://bphc.hrsa.gov/programopportunities/fundingopportunities/SAC/index.html

Authority: Public Health Service Act, Section 330, as amended (42 U.S.C. 254b)

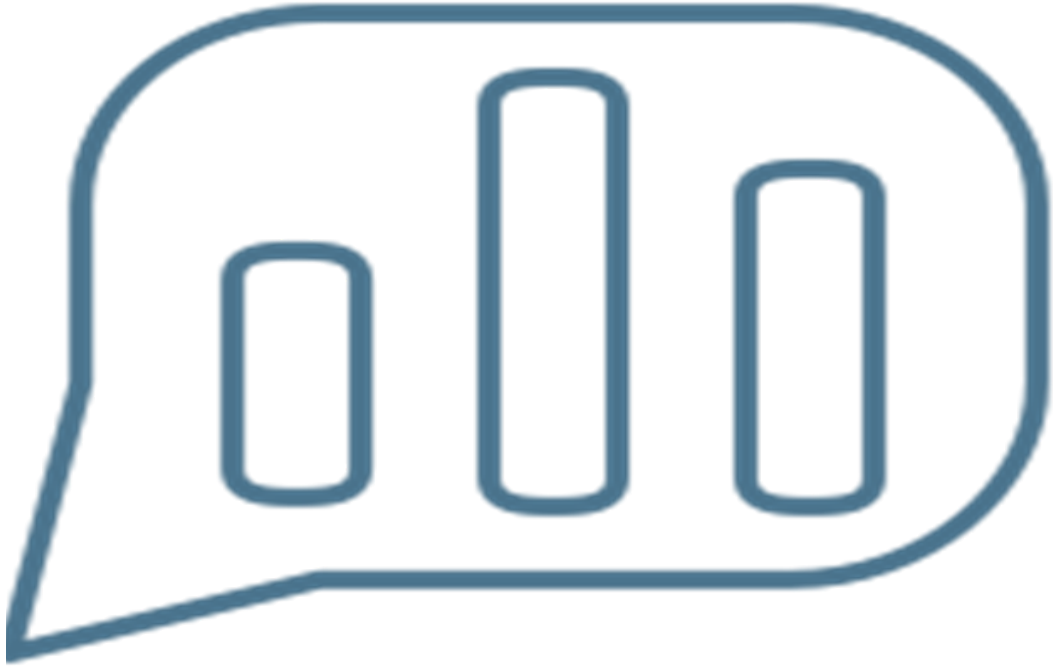
** Including natural or manmade disasters, as well as emergent or established public health emergencies.*

# Additional Requirements

- The Joint Commission
- AAAHC (Accreditation Association for Ambulatory Health Care)
- Other applicable requirements

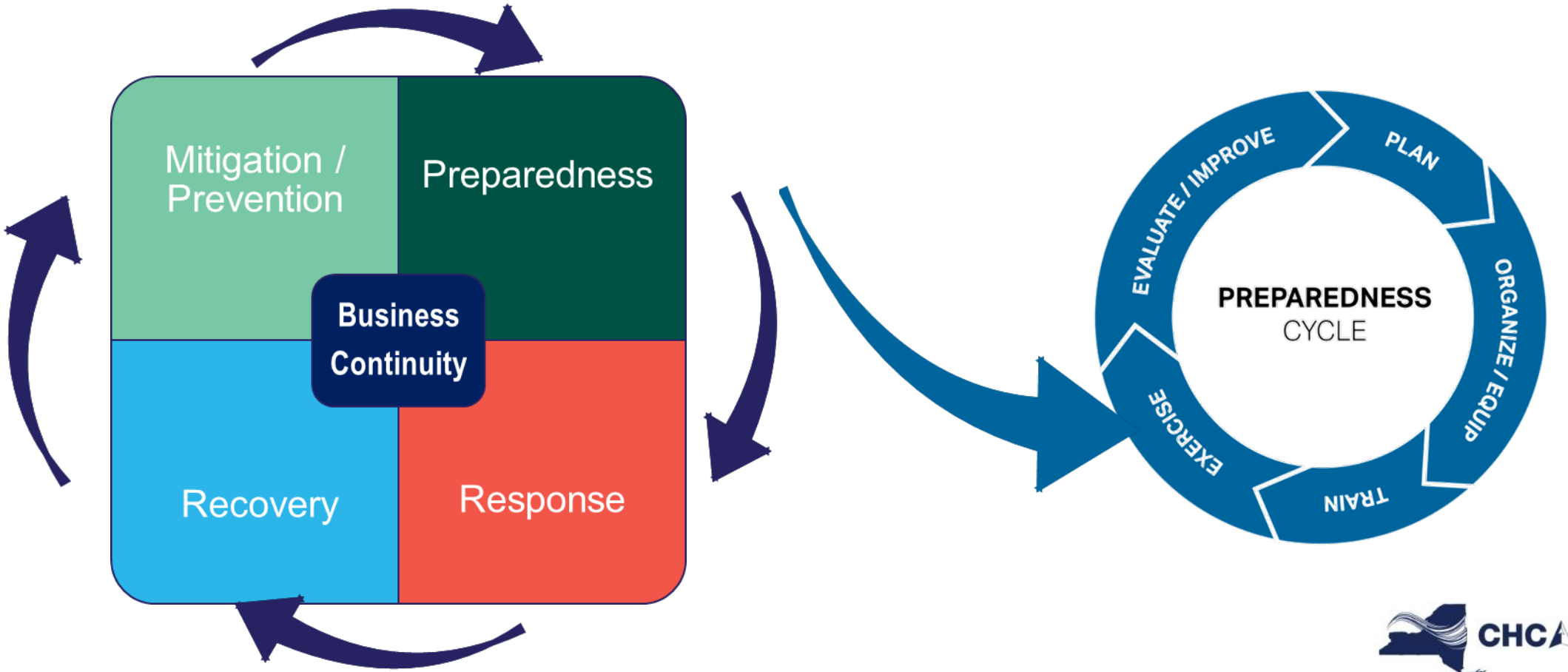
# Participant Poll

Does your organization include Information Technology/Information Systems (IT/IS) staff in emergency preparedness (EP) activities?



# Comprehensive Emergency Management Program (CEMP)

A CEMP is based on the 4 phases of Emergency Management (EM).



# CEMP: It Takes a Village

- A robust CEMP requires the expertise and commitment of a multidisciplinary team from across the health center.
- Information Technology (IT)/Information Systems (IS) staff MUST be part of the EM Team at your health center.

# Emergencies and Disasters Don't Care About Silos

- Security breaches and loss of IT/IS capabilities are NOT just "IT's problem."
- Considerations for cybersecurity and Information Technology (IT)/Information Systems (IS) MUST be part of your organization's risk assessment, mitigation initiatives, preparedness planning, and response structure.


"Total anarchy always breaks out when we have computer problems."

# OK, I know we need to plan for cybersecurity and loss of IT/IS capabilities, *but*…

**Where do we start?**

Business Continuity

Regulatory Requirements

Cybersecurity

Ransomware

All Hazards

Emergency Management

Preparedness Cycle

Risk Assessment

Viruses

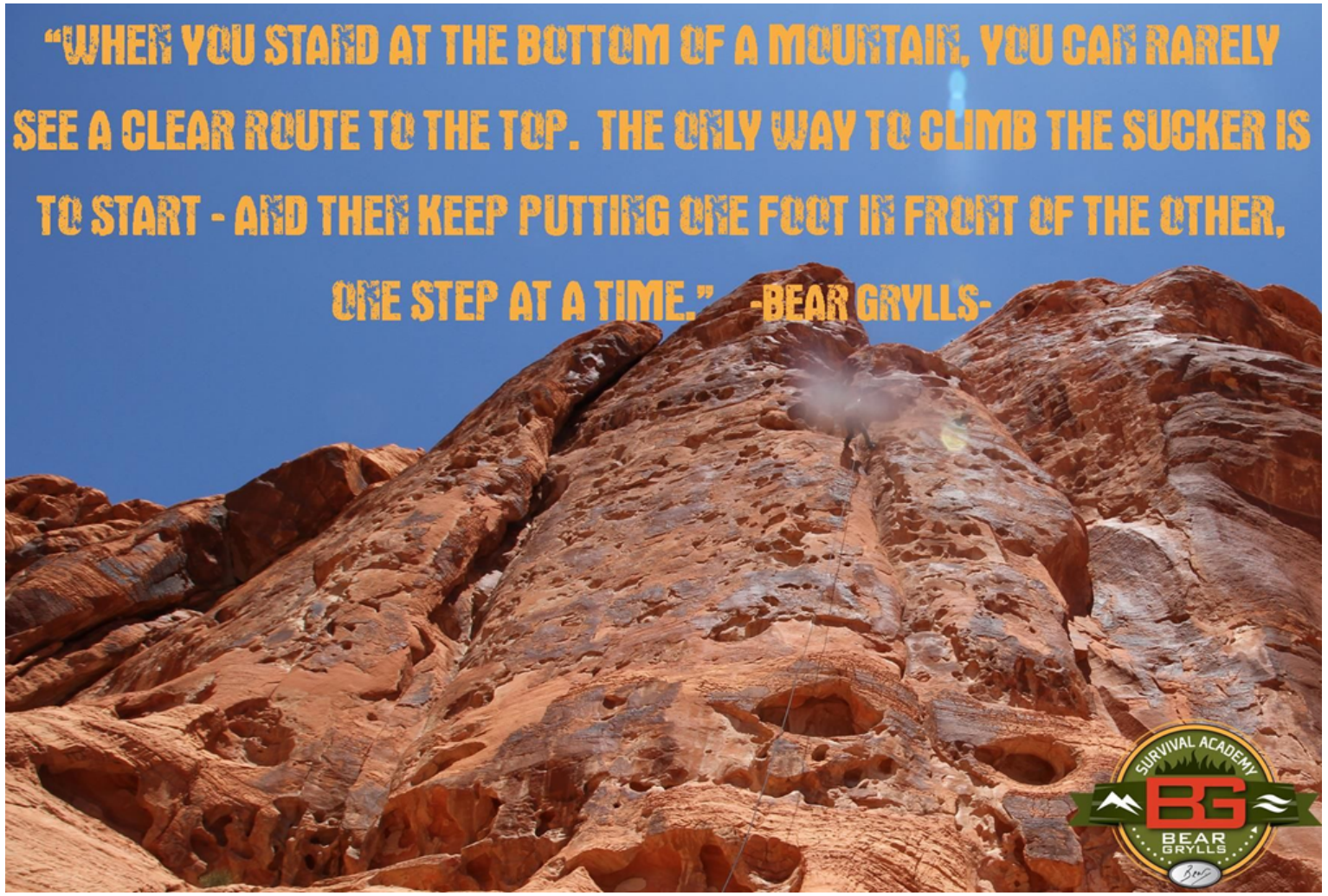
Mitigation

Response Plan

Multidisciplinary Committee

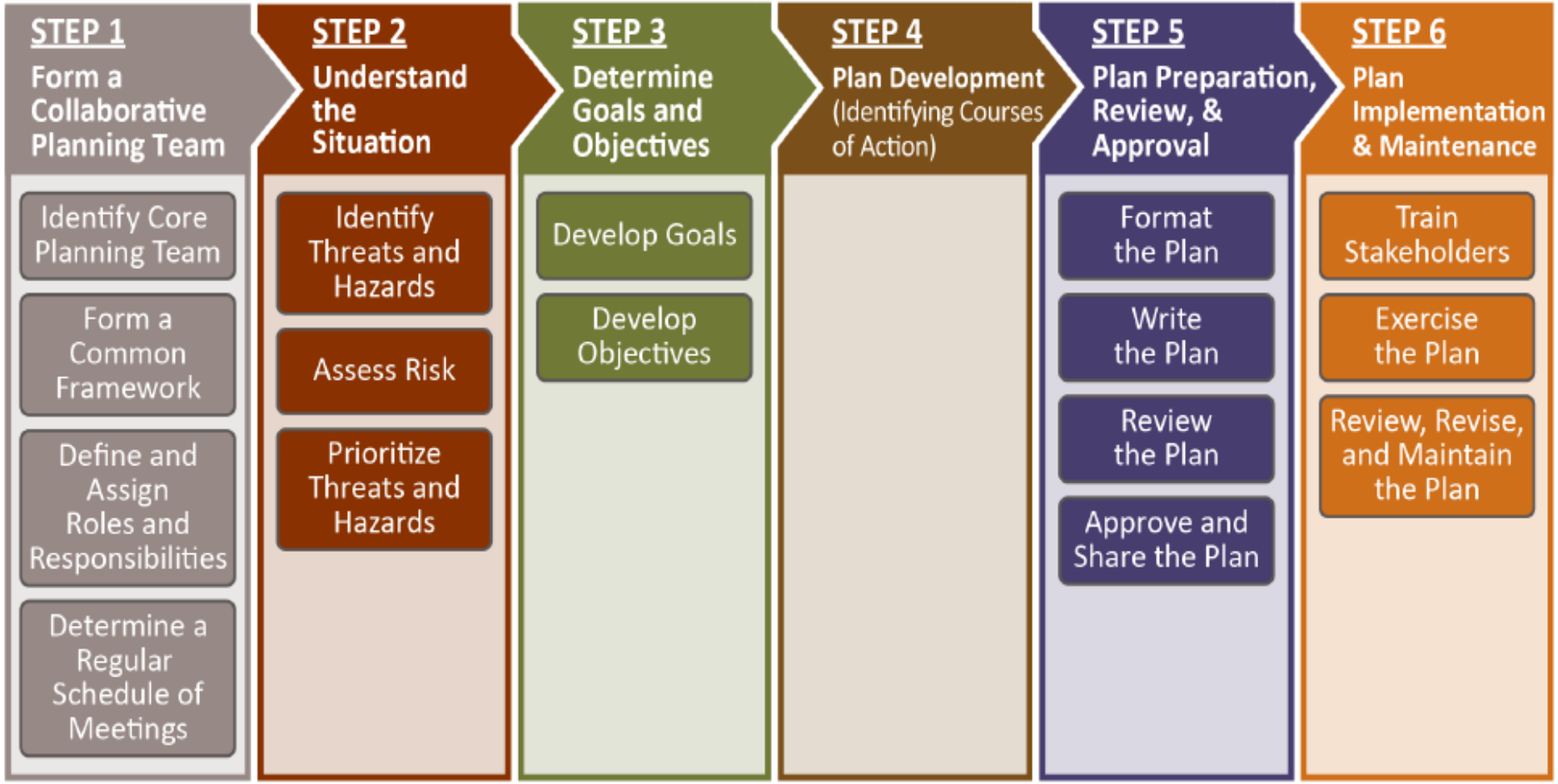
Recovery

# You Just Start!




(There are tools to help!)

# The EM Planning Process: Don't Forget IT




Source: FEMA

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

# Best Practice: Risk Assessment Should Guide Planning

- Risk assessment is an ongoing preparedness activity.
  - Risk assessment should be annual.
  - Multidisciplinary EM Committee members should work together to conduct risk assessment.
  - Consult local and state public health risk analyses, as well as jurisdictional risk analyses to inform your organizational risk assessment.
  - Ensure the assessment team works within a common frame of reference, with clearly defined scenarios and assumptions for scoring risk.
  - Consider hiring or designating a Chief Information Security Officer (CISO).

# Risk Assessment Basics

Risk= Severity/Magnitude x Probability

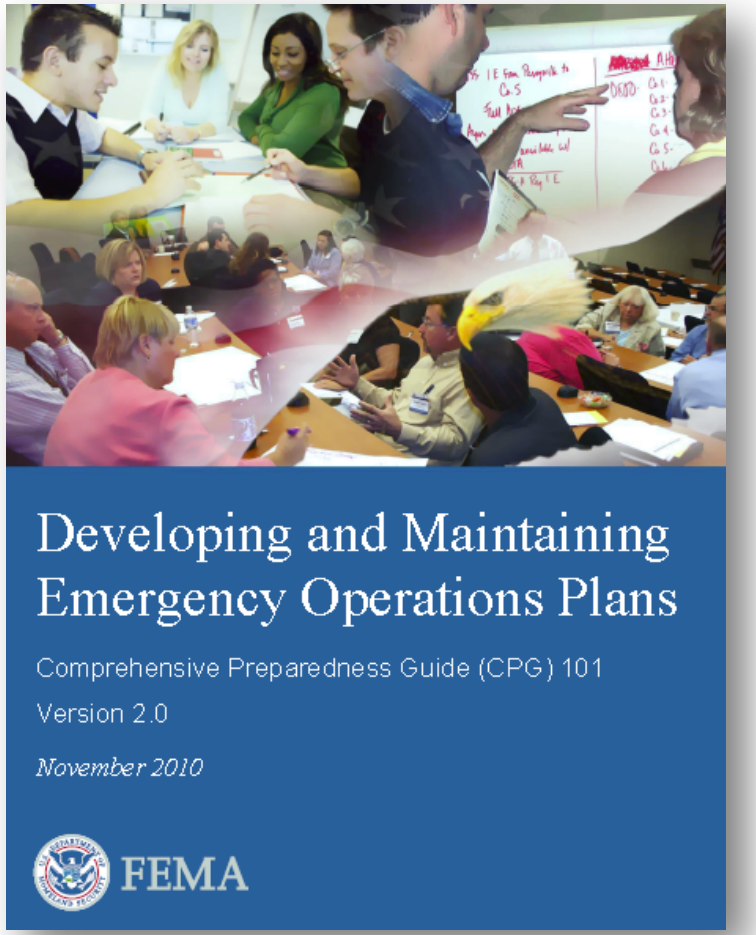
- Be proactive-Know what data and information you have that's worth protecting and identify the risk that comes along with that.
  - Consider both known and projected risks.
  - Use data from actual occurrences or studies, when possible.
- Risk is relative compared to other hazards, not absolute.

# Risk Analysis Tools and Resources

- Kaiser Permanente Hazard Vulnerability Analysis (HVA) Tool includes multiple hazards and assesses risk by probability; potential or known magnitude/impact; and mitigation actions.
  - Current version (2017) includes considerations for real alerts/activations.
- HHS Guidance on Risk Analysis provides information on the requirements of the HIPAA Security Rule; key considerations for risk analysis; and key steps in conducting a risk analysis.
- The Security Risk Assessment Tool from HealthIT.gov is more specific to assist small and medium-sized health care practices and business associates in complying with the HIPAA Security Rule.

# Create an All-Hazards Emergency Operations Plan (EOP)

- Base Plan should be generalized
  - Intro, Purpose, emergency Command and Control, 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.



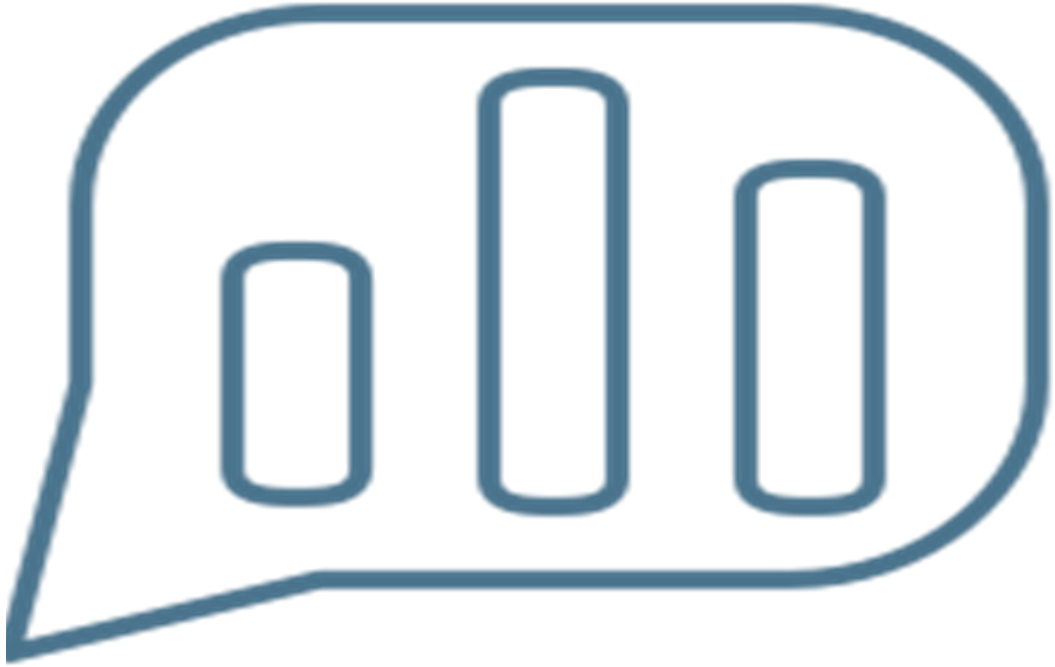

https://www.fema.gov/pdf/about/divisions/npd/CPG_101_V2.pdf

# All-Hazards Base Plan vs. Cybersecurity-Related Policies & Procedures

- The EOP base plan should contain key information that generally applies to all potential hazards.
- Cybersecurity-related policies & procedures should be detailed in a hazard-specific annex to the All-Hazards EOP.
  - The annex should include provisions based on the guidance contained in the Cybersecurity Framework.

# Participant Poll

Does your organization have a written hazard-specific plan for Cyberattack and loss of Information Technology/ Information Systems (IT/IS) as part of its All-Hazards Emergency Operations Plan (EOP)?

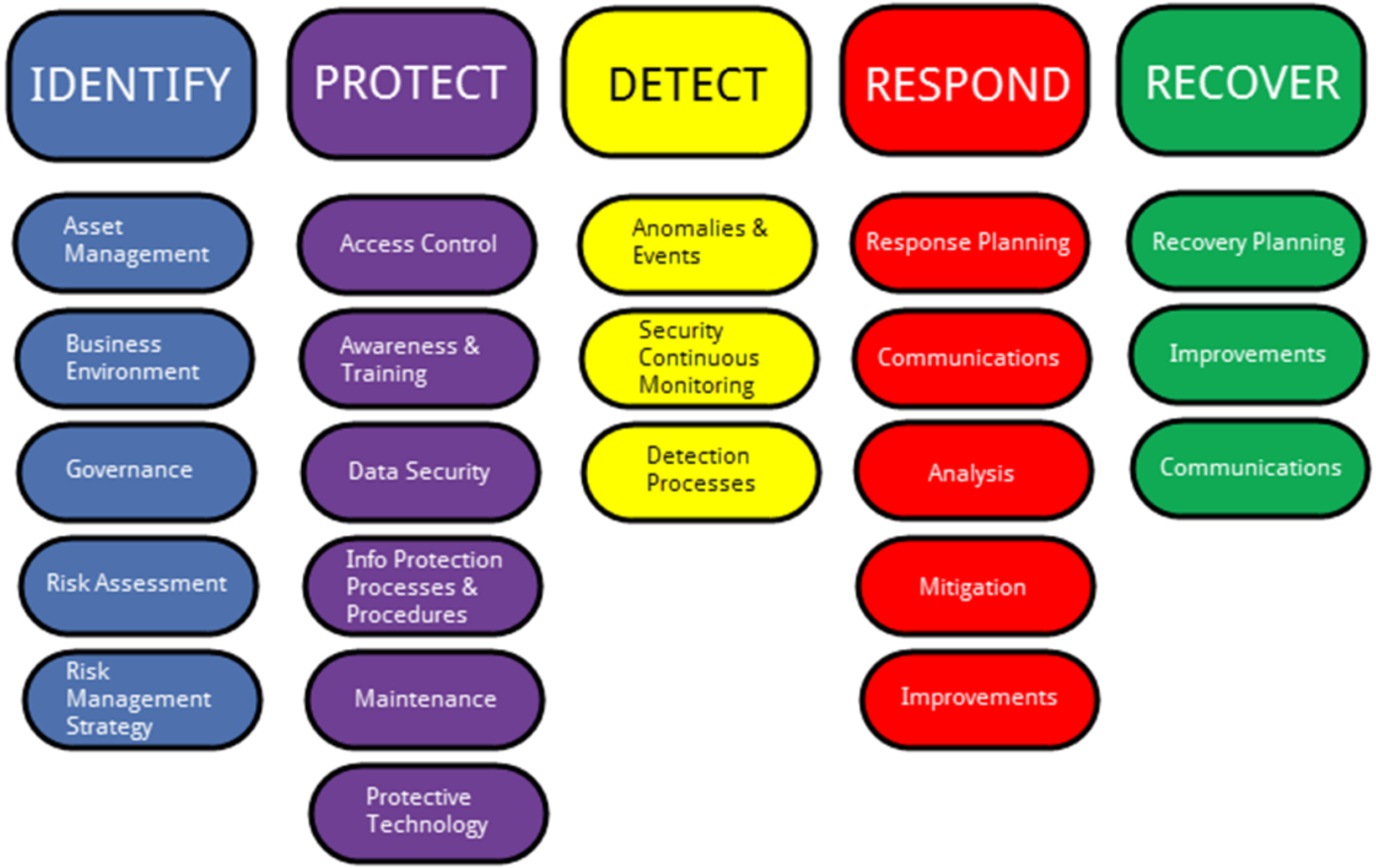


# Cybersecurity Framework

- The Cybersecurity Framework is a set of guidelines for private sector companies to follow to be better prepared in identifying, detecting, and responding to cyber-attacks.
- **The five functions represent the primary pillars of a successful and holistic cybersecurity program.**


https://www.nist.gov/cyberframework

# Cybersecurity Framework Overview



# Framework Core Function

Identify - Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.

- Examples of outcome Categories within this Function include:
  - Asset Management
  - Business Environment
  - Governance
  - **Risk Assessment***
  - **Risk Management Strategy***

# Resource – Health Industry Cybersecurity Practices

- Aims to raise awareness, provide vetted cybersecurity practices, and move towards consistency in mitigating the current most pertinent cybersecurity threats to the sector. It seeks to aid healthcare and public health organizations to develop meaningful cybersecurity objectives and outcomes.
  - The **main document** examines cybersecurity threats and vulnerabilities that affect the healthcare industry. It explores (5) current threats and presents (10) practices to mitigate those threats.
  - ***Technical Volume 1*** discusses these ten cybersecurity practices for small healthcare organizations
  - ***Technical Volume 2*** discusses these ten cybersecurity practices for medium and large healthcare organizations.
  - ***Resources and Templates*** volume provides additional cybersecurity resources and references

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

# Framework Core Function

Protect – Develop and implement appropriate safeguards to ensure delivery of critical services.

- Examples of outcome Categories within this Function include:
  - Identity Management and Access Control
  - **Awareness and Training***
  - Data Security
  - Information Protection Processes and Procedures
  - Maintenance
  - Protective Technology

# Training and Exercises Must be Conducted

- Homeland Security Exercise and Evaluation Program (HSEEP) provides guidance.
- Online training is available through the Emergency Management Institute (EMI).
- Tools and Templates are available to assist with:
  - Creating a Training and Exercise Plan (TEP);
  - Designing, conducting, and evaluating discussion-based and operations-based exercises; and
  - After-action reporting and improvement planning.

https://www.fema.gov/emergency-managers/national-preparedness/exercises/hseep

# Exercises—Key Points

- Make sure that all participants have been TRAINED on *documented* plans.
  - Exercises should be based on current capabilities, and not "wishful thinking."
- Include leadership in the design and conduct of the exercise to demonstrate organizational commitment.
- Include stakeholders from across the organization, as well as contracted vendors supporting your organization's cybersecurity and IT/IS infrastructure.
- Be sure to evaluate each exercise and devise an improvement plan.

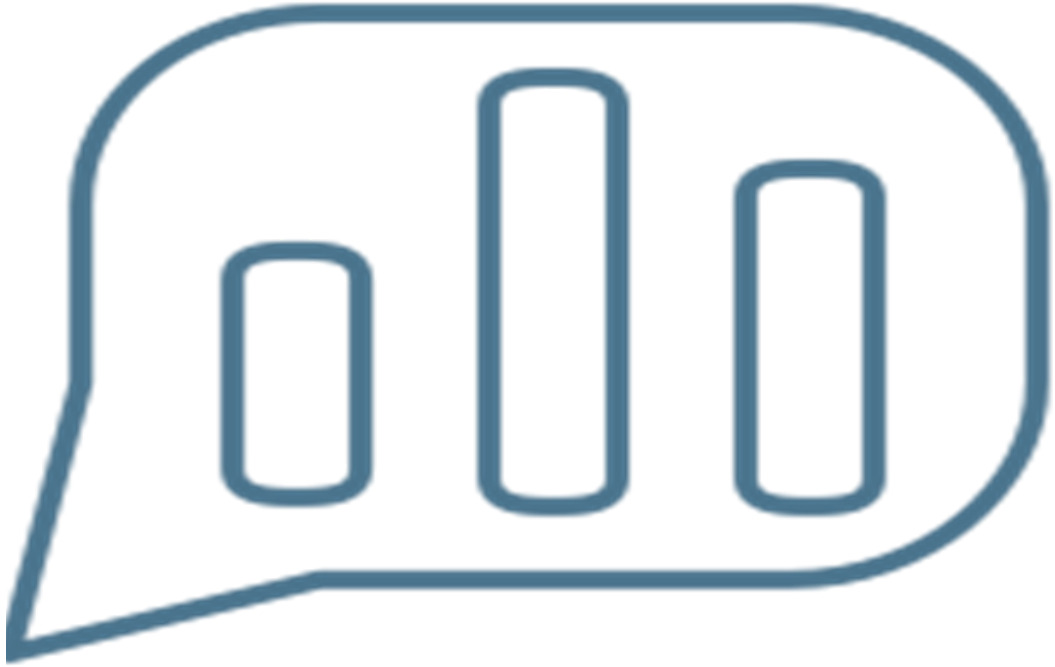
**If your organization experiences a real-world emergency, document lessons learned and update plans accordingly.*

# Start With a Tabletop Exercise That Simulates a Cyber Incident

- Focus on detection, incident management and response, and recovery.
- Evaluate completeness of plans and decision-making readiness.
- Identify gaps and define ways to address them through improvement planning.
- If your organization outsources certain functions, identify involved stakeholders and their respective roles and responsibilities.
  - Focus on "high risk" data.

# Participant Poll

Has your organization tested and evaluated your plans for a Cyberattack and loss of Information Technology/ Information Systems (IT/IS) and/or experienced and responded to an attack resulting in loss of its Information Technology/Information Systems (IT/IS) within the past 3 years?



# Framework Core Function

Detect – Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.

- Examples of outcome Categories within this Function include:
  - Anomalies and Events.
  - Security Continuous Monitoring.
  - Detection Processes.

# Framework Core Function

Respond – Develop plans and implement appropriate actions against a detected cybersecurity incident.

- Examples of outcome Categories within this Function include:
  - Response Planning
  - **Communications***
  - Analysis
  - **Mitigation***
  - **Improvements***

# HRSA Emergency Reporting Expectations

HRSA Health Center Program

## Primary Health Care Digest

**September 3, 2019**

**Hurricane Dorian Reporting**
HRSA will ask Primary Care Associations (PCAs) to take the lead in gathering critical health center information and reporting impact data back to us on the operational status of delivery sites. Read the bulletin we sent last week. For health centers in areas impacted by Hurricane Dorian (i.e., Florida, Georgia, and South Carolina), we ask that you report site-level operational status to your PCA.

Please also
important
temporary
including v
page for
scope for
ncy events,

### Health Center COVID-19 Survey

**COVID-19 Health Center Survey Testing Dashboard**

Visit a dashboard on COVID-19 testing broken down by race/ethnicity.

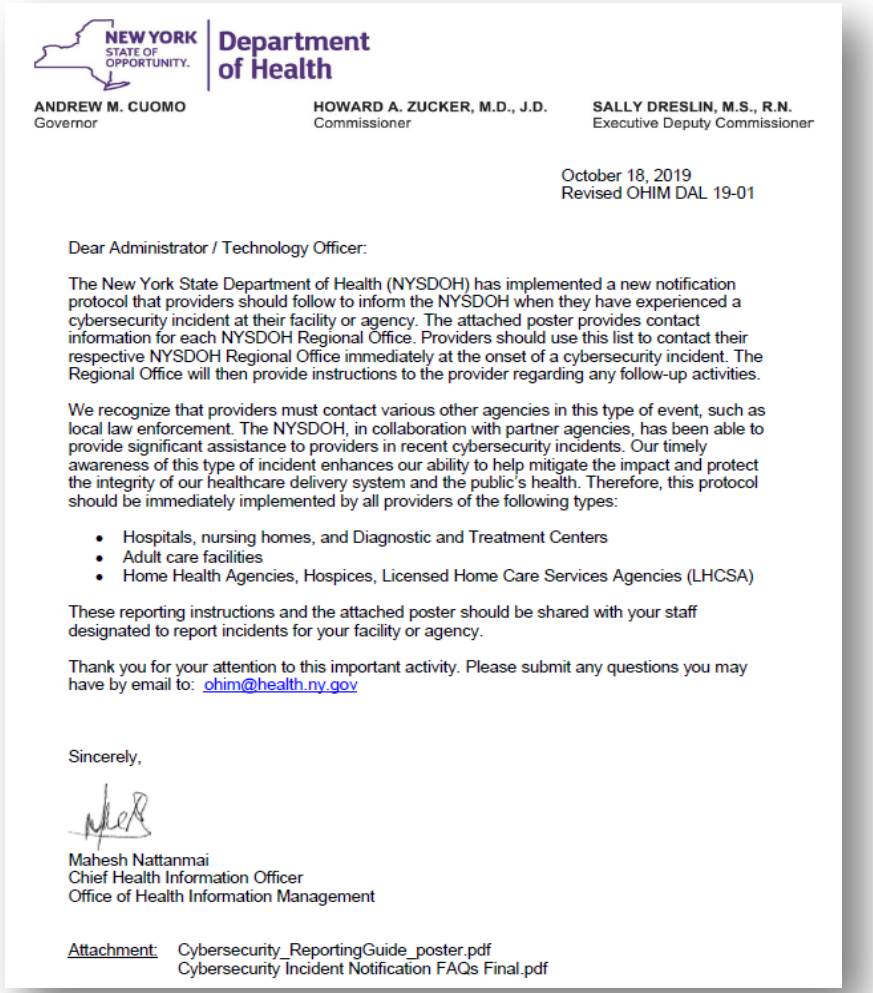
**COVID-19 Health Center Survey Maps**

View maps of the COVID-19 survey data, including testing capacity, temporary site closures, and staff ability to work.



CHCANYS

# Contact Your NYSDOH Regional Office Immediately If You Detect a Cybersecurity Incident



NEW YORK STATE OF OPPORTUNITY. Department of Health

ANDREW M. CUOMO
Governor

HOWARD A. ZUCKER, M.D., J.D.
Commissioner

SALLY DRESLIN, M.S., R.N.
Executive Deputy Commissioner

October 18, 2019
Revised OHIM DAL 19-01

Dear Administrator / Technology Officer:

The New York State Department of Health (NYSDOH) has implemented a new notification protocol that providers should follow to inform the NYSDOH when they have experienced a cybersecurity incident at their facility or agency. The attached poster provides contact information for each NYSDOH Regional Office. Providers should use this list to contact their respective NYSDOH Regional Office immediately at the onset of a cybersecurity incident. The Regional Office will then provide instructions to the provider regarding any follow-up activities.

We recognize that providers must contact various other agencies in this type of event, such as local law enforcement. The NYSDOH, in collaboration with partner agencies, has been able to provide significant assistance to providers in recent cybersecurity incidents. Our timely awareness of this type of incident enhances our ability to help mitigate the impact and protect the integrity of our healthcare delivery system and the public's health. Therefore, this protocol should be immediately implemented by all providers of the following types:

- Hospitals, nursing homes, and Diagnostic and Treatment Centers
- Adult care facilities
- Home Health Agencies, Hospices, Licensed Home Care Services Agencies (LHCSA)

These reporting instructions and the attached poster should be shared with your staff designated to report incidents for your facility or agency.

Thank you for your attention to this important activity. Please submit any questions you may have by email to: ohim@health.ny.gov

Sincerely,

Mahesh Nattanmai
Chief Health Information Officer
Office of Health Information Management

Attachment: Cybersecurity_ReportingGuide_poster.pdf
Cybersecurity Incident Notification FAQs Final.pdf

- State Department of Health (SDOH) notification protocol for when providers have experienced a potential cyber security incident at their facility or agency.
- Issued by Office of Health Information Management (OHIM DAL 19-01) on August 12, 2019 and in effect immediately.
- Update issued by Office of Health Information Management (Revised OHIM DAL 19-01) on October 18, 2019. Includes a FAQ sheet.
- For questions: Please send an e-mail to ohim@health.ny.gov

# SDOH Cybersecurity Protocol (cont.)

## Business Hours

8:30 am to 4:45 pm weekdays and non-holidays, unless noted

| | |
|---|---|
| **Capital District**<br>Albany, Clinton, Columbia, Delaware, Essex, Franklin, Fulton, Greene, Hamilton, Montgomery, Otsego, Rensselaer, Saratoga, Schenectady, Schoharie, Warren and Washington | (518) 402-1036 |
| **Central New York**<br>Broome, Cayuga, Chenango, Cortland, Herkimer, Jefferson, Lewis, Madison, Oneida, Onondaga, Oswego, St. Lawrence, Tioga and Tompkins | (315) 477-8400 |
| **Metropolitan Area**<br>9:00 am to 5:00 pm<br>Bronx, Kings, New York, Queens and Richmond | (212) 417-5550 |
| **Central Islip**<br>9:00 am to 5:00 pm<br>Nassau and Suffolk | (631) 851-8050 |
| **New Rochelle**<br>9:00 am to 5:00 pm<br>Dutchess, Orange, Putnam, Rockland, Sullivan, Ulster and Westchester | (914) 654-7005 |
| **Western Area**<br>Allegany, Cattaraugus, Chautauqua, Chemung, Erie, Genesee, Livingston, Monroe, Niagara, Orleans, Ontario, Schuyler, Seneca, Steuben, Wayne, Wyoming and Yates | (716) 847-4505 |

## After Hours Emergencies

4:45 pm to 8:30 am weekdays. Available 24 hours a day on weekends and holidays.

| | |
|---|---|
| **NYSDOH Duty Officer**<br>Select option #1 for reporting an emergency. | (866) 881-2809 |

**CALL 911 if there is immediate threat to public health or safety.**

In all cases, the cybersecurity incident should be reported to law enforcement.

## You're the Key to Reporting a Cybersecurity Incident!

**An incident is considered a reportable "cybersecurity incident" under the New York State Department of Health guideline, if it affects patient care, or represents a serious threat to patient safety, including intrusions whose intent appears to be breach or theft of protected health records. Examples include, but are not limited to:**

a. Successful intrusions into a health care provider's information technology system (including those that are contracted out by the health care provider), network infrastructure, and/or medical equipment/devices.

b. Ransomware attacks that disable all or part of information technology operations including administrative systems such as payroll, billing, or appointment scheduling.

c. Cybersecurity incidents that have the potential to spread through established connections to other health care networks or government systems. Examples include file transfer systems or data reporting interfaces.

# What is the Role of the State Health Department?

- Engage with the provider to learn and assess the impact of the cyber event to the larger public health landscape.
- Facilitate communication with State, Federal and third-party resources as the need arises.
- Advise providers of alternative methods of continuing critical aspects of their operations during an IT outage.
- Collect and share general information on the cyber threats with other providers to prevent and protect other providers from similar vulnerabilities.
- Establish and maintain a trusted collaboration with all types of providers, associations, other stakeholders.
- Liaise with Health Information Technology community as needed.
- Protect State IT resources as necessary.

# GNYHA Guide to Cybersecurity Reporting

**RESPOND: Based on the specifics of the attack on your facility, consider the following actions.**

| CYBER ACTIVITY TYPE | RECOMMENDED ACTION | AGENCY/ GOVERNANCE | |
|---|---|---|---|
| Has the cyber activity impacted medical devices? | Report cybersecurity incidents through the Food and Drug Administration's (FDA) "Medical Device Reporting" (MDR) system. User facilities are required to report device-related deaths to the FDA and the associated manufacturer within 10 working days of when they became aware of the incident. | FDA | |
| Was there a breach of protected health information or other private information? | Refer to *HIPAA Breach Notification Rule*, 45 CFR §§ 164.400-414 to determine if breach reporting is necessary per the Office for Civil Rights (OCR) guidance.<br>• OCR's most recent cyber guidance<br>• OCR's most recent ransomware guidance | OCR | FBI |
| | New York State Information Security Breach and Notification Act comprised of section 208 of the State Technology Law and section 899-aa of the General Business Law stipulates breach reporting requirements to certain State agencies by faxing a data breach form. The Act applies to breaches of "private information," defined as any personal information concerning a natural person in combination with any one or more of the following data elements: social security number, driver's license number, account number, or credit or debit card number in combination with any required security code. | New York State Police | |
| | | New York State Attorney General's Office | • Fax: 212-416-6003<br>• E-mail: breach.security@ag.ny.gov |
| | | New York State Department of State | Division of Consumer Protection<br>Attn: Director of the Division of Consumer Protection<br>Security Breach Notification<br>• Consumer Assistance: 518-474-8583<br>• Fax: 518-473-9055<br>• E-mail: security_breach_notification@dos.ny.gov |

**FBI New York Regional Cyber Branch** (New York City, Nassau, Suffolk, Westchester, Putnam, Orange, and Rockland counties)
Phone: 212-384-2023

**Albany Regional Office**
Phone: 518-465-7551

**Buffalo Regional Office**
Phone: 716-865-7800

**Newark Regional Office** (Covers majority of New Jersey)
Phone: 973-792-3015

- View additional regional FBI offices.
- File a complaint with the FBI Internet Crime Complaint Center.



CHCANYS

# Contact CHCANYS

- As soon as you are able, contact CHCANYS so the EM Team can maintain situational awareness (emteam@chcanys.org).
- As the state Primary Care Association, HRSA will often request information from CHCANYS.
- CHCANYS is better able to assist you, when possible, if the EM Team is aware of your emergency.

# Mitigate! Healthcare Sector Attacks Can Spread Very Quickly

- May cause major disruption of the healthcare delivery system in a city, county, or region, involving thousands of providers, patients and residents:
  - Interconnected/interdependent provider networks and communications between referring providers deliver multiple access points for attack;
  - Disparity between organizations' ability to address cybersecurity issues—the health care sector will only be as secure as the weakest link;
  - Locations not expecting to be a target can serve as doorways to other, more complex partners with greater cyber risks and rewards for the hacker.

# Stay Current With Cybersecurity Guidance and Advisories


https://www.chcanys.info/covid-guidance/categories/cybersecurity



CHCANYS

# Homeland Security Cybersecurity Advisors

- The Department of Homeland Security's (DHS) Cybersecurity Advisor (CSA) Program offers cybersecurity assistance on a voluntary, no-cost basis to critical infrastructure organizations.
- The CSA Program maintains regional subject matter experts throughout DHS emergency management and protection regions. CSAs introduce organizations to various no-cost DHS cybersecurity products and services, along with other public and private resources, and act as liaisons to other DHS cyber programs and leadership.

**DHS Region II Cybersecurity Advisor (CSA)**

R. S. Richard Jr.

richard.richard@hq.dhs.gov

(631) 241-3662

# Framework Core Function

**Recover** – Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

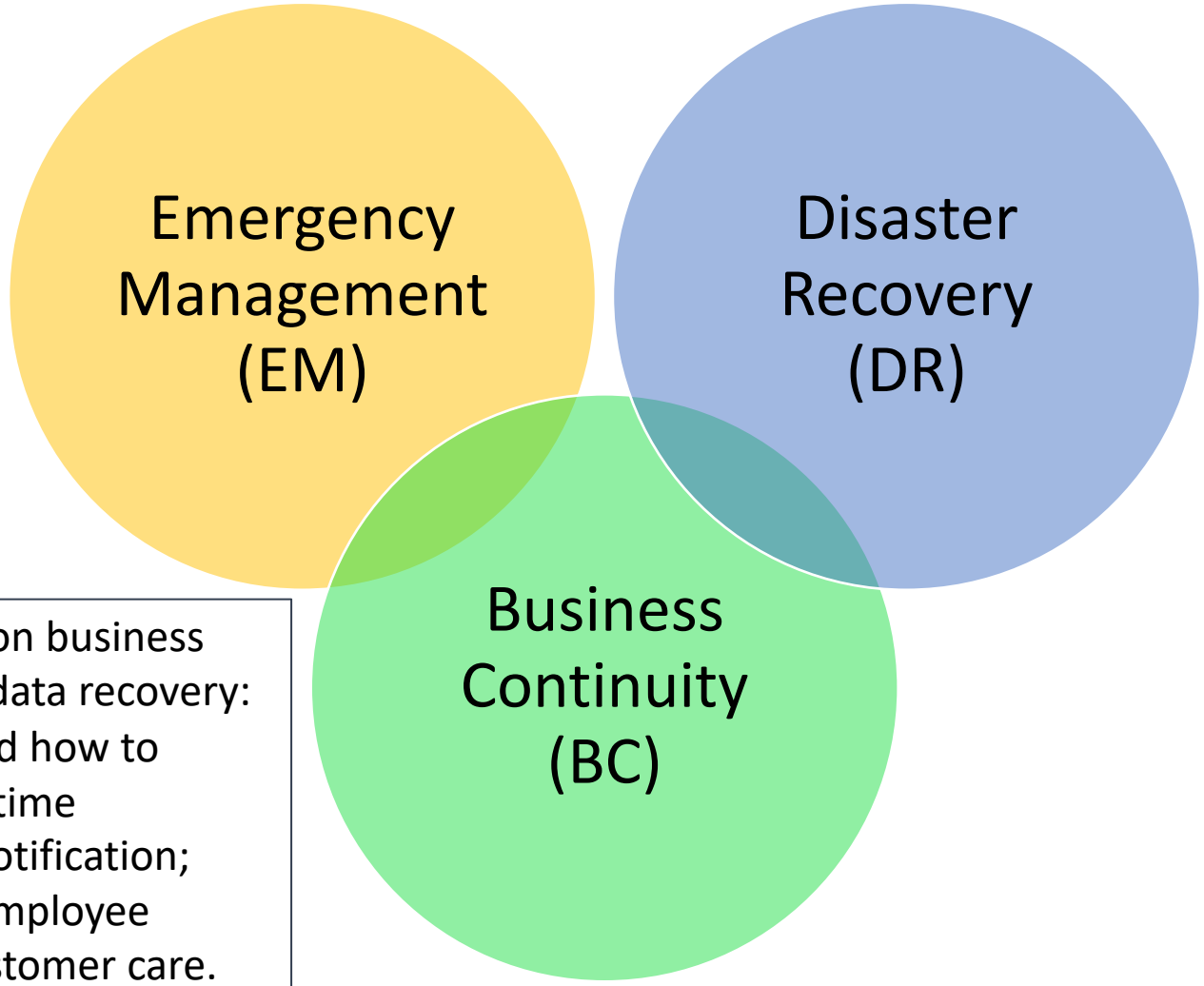
- Examples of outcome Categories within this Function include:
  - Recovery Planning
  - Improvements
  - Communications

# Business Continuity Plans Help Your CHC Maintain Operations

- How will your CHC manage the loss of your EMR?
- How will the data collected and recorded be entered into the EMR upon its recovery?
- How will billing, timekeeping, and payroll be managed during response and recovery?
- What redundancies are available for compromised Internet-based communications systems?
- How will you manage security if physical access control mechanisms are impacted by an incident?

# EM+BC+DR=Successful Response

EM provides the "all-hazards" structure and organization to respond to any emergency.



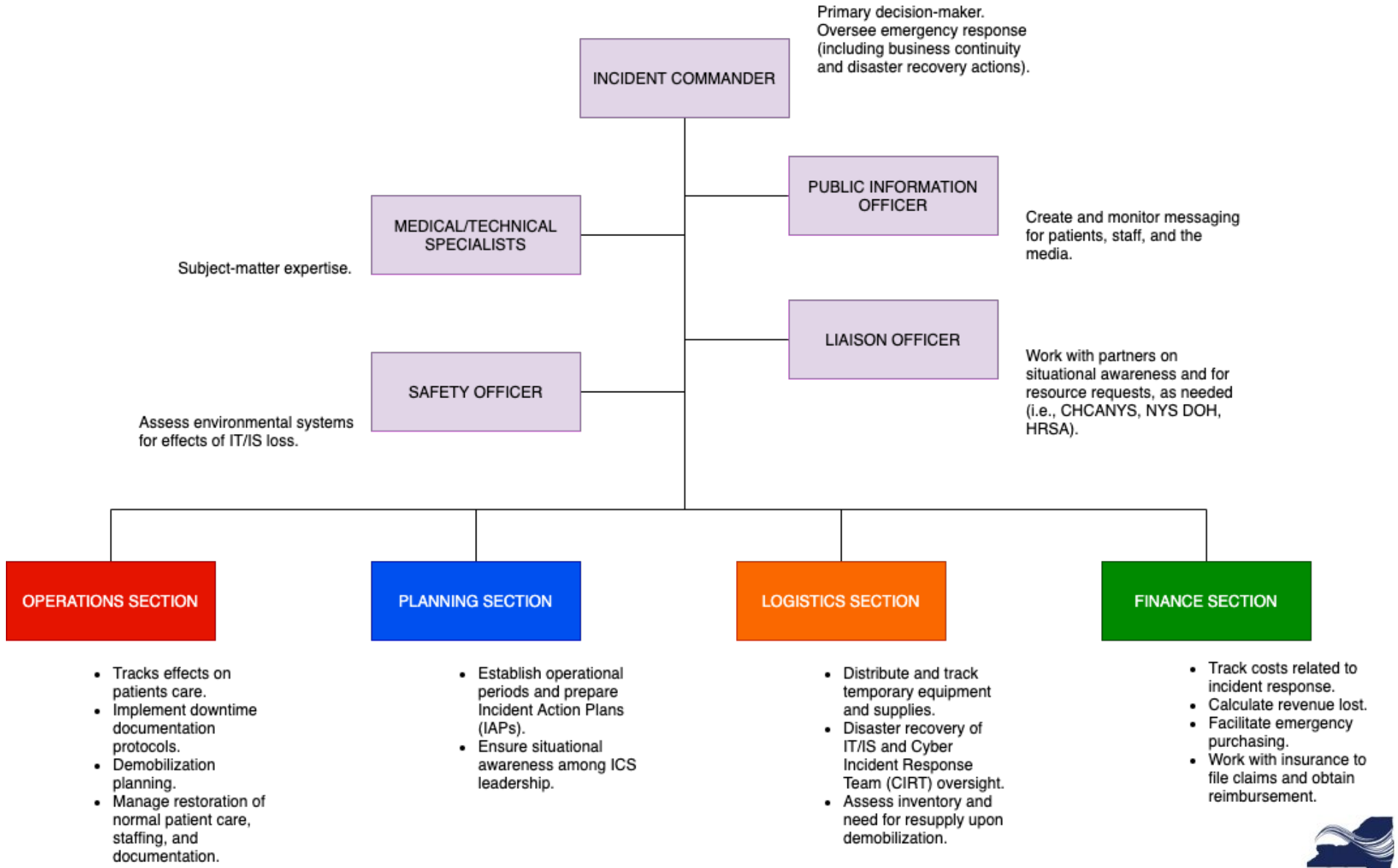

DR is usually centered around the IT areas of an organization: recovering servers or mainframes; re-establishing private brand exchanges; or provisioning local area networks to meet critical business function needs.

BC generally focused on business operations vs. IT and data recovery: essential functions and how to maintain them; downtime procedures; vendor notification; asset management; employee management; and customer care.

# Define a Command and Control Structure to Manage Response and Recovery

- Cybersecurity incident response and recovery must be accounted for in your organization's Incident Command System (ICS) structure.
  - A cybersecurity incident may impact different facets of your health center's operations.
  - Response strategy and tactics should be based on a Common Operating Picture—all decision-makers need to have the same understanding of the situation to direct response and recovery actions.

# ICS and Cybersecurity Response and Recovery

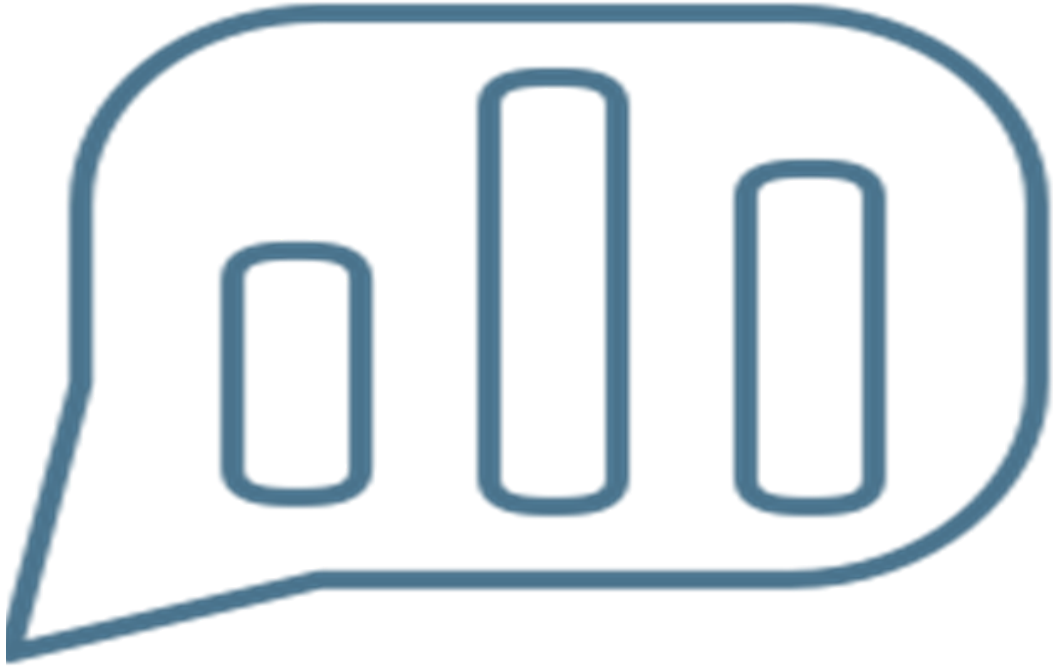


# Mini Discussion

- Who from your organization would you put into the Medical-Technical Specialists Role when responding to a Cybersecurity incident?
- Does this expertise exist within your health center?

# Participant Poll

Are your organization's Information Technology/ Information Systems (IT/IS) staff assigned to an Incident Command System (ICS) role and have they been trained in that role?



# Activity

- Categorize sample incident action objectives for cyber incident response as being part of Business Continuity, Disaster Recovery, or Emergency Management.

# EM vs. BC vs. DR

- Activate EOP, Security Incident Response Plan, ICS, EOC.
- Consider limiting or ceasing nonessential services.
- Prepare initial risk comms. for staff and patients.
- Contact local LE, FBI, NYS DOH, and CHCANYS.
- Implement downtime documentation and critical diagnostic and support systems protocols to maintain pt. care.
- Assess degree of IT/IS breach and disruption; recommend interim corrective actions.
- Establish operational periods and incident objectives.
- Collect and collate manual incident documentation.
- Isolate and repair, replace, or remove affected systems from the network.
- Provide for integrity of system backup data and plan for system restoration.
- Implement manual inventory and resupply processes.
- Update patients and staff on situation status.
- Update local EM, NYS DOH, and HRSA on incident response.
- Update incident objectives with new info and intelligence.
- Implement manual staff timekeeping and scheduling.
- Prepare for demobilization and system recovery.
- Provide resources for alternate doc. systems
- Monitor systems for new threats.
- Plan for migration of manual documentation to electronic processes upon restoration.
- Consider alternate methods to ensure payroll processing.
- Track incident response hours.
- Monitor and track costs related to disruption of IT/IS.
- Restore patient care and management activities.
- Notify Legal and Risk Mgmt. of actual or potential PHI compromises or violations.
- Write AAR.
- Inventory supplies for EOC and pt. care and replenish
- Document recommendations for updating and improving diagnostic and cyber protective services.
- Compile final summary of response and recovery costs and estimated lost revenue.
- Work with insurance carrier for reimbursement and claims procedures.

# Final Thoughts

- A health center's CEMP must include preparedness, mitigation, response, and recovery considerations for a cybersecurity incident.
  - IT/IS staff responsible for security should be part of the multidisciplinary Emergency Management (EM) Team.
  - A Security Incident Response Plan Annex should be developed as part of the EOP.
  - ALL health center staff must be trained in cyber safety protocols, and in protocols for continuation of patient care and other essential functions if IT/IS are lost due to a security incident.
- EM, business continuity (BC), and disaster recovery (DR) planning are complementary—all are needed for successful response to a cybersecurity incident.

# Thank You!