Pennsylvania
Department of Human Services



ICF Taskforce Meeting - October 2026

Prepared People Save Lives

The Value Proposition



Being prepared - it's a smart choice that **protects people**, **saves money,** and helps your organization **stay safe and trustworthy.**

Everyday Lives and Prepared People.

Our Objectives Today

- October is Cybersecurity Awareness Month
- 4 Easy Ways to Stay Safe Online
- Building a Strong Cybersecurity Culture
- Evacuation and Shelter-In-Place Communities of Practice Webinar
- High Utility Exercises “Ready out of the Box” Discussions
- The Extended Cyberattack TTX



Cyber Intrusion or Bad Actor Mitigation Tactics

4 Easy Ways to State Safe Online

- Use Strong Passwords and a Password Manager
- Turn on Multifactor Authentication
- Recognize and Report Phishing Attacks
- Update Your Software







Building a Strong Cybersecurity Culture

- **Use basic cybersecurity training.** This helps familiarize staff with cybersecurity concepts and activities associated with implementing cybersecurity best practices.
- **Identify available cybersecurity training resources.** Cybersecurity training resources—on topics like phishing and good email practices—are available through professional association, educational institutions, as well as private sector and government sources.
- **Stay current on cybersecurity events and incidents.** This helps identify lessons learned and helps to maintain vigilance and agility to cybersecurity trends.
- **Encourage employees to make good choices online** and **learn about risks** like phishing and business email compromise.

Cybersecurity Training

Training & Grant Programs

- **Training - No-cost FEMA-funded cybersecurity courses: https://nationalcpc.org/**
  The program is also always looking for new host sites.
- **No-cost virtual Introduction to Community Lifelines course: https://training.fema.gov**
- **FEMA State and Local Cybersecurity Grant Program: https://www.fema.gov/grants/preparedness/state-local-cybersecurity-grant-program**

Evacuation and Shelter-in-Place COP Webinar

Upcoming Evacuation and Shelter-in-Place - Community of Practice Webinar

- **Date: November 17, 2026**
- **Time: 2:00 PM – 3:30 PM ET**
- **Registration Link: Zoom**

Federal Emergency Management Agency's Out of Harm's Way: Evacuation and Shelter-in-Place Program is pleased to invite you to our Community of Practice (COP) webinar scheduled for Tuesday, November 17, 2026. This webinar builds on the technical discussions and peer-to-peer learning that is hallmark to the *Out of Harm's Way Technical Assistance* (TA) program. This webinar will allow speakers to analyze and hone in on the more granular realities of real-world evacuations and shelter-in-place events.

High-Utility Exercises ("Ready To Go" Out of the Box)



- **Strengthening Readiness Through Practical Discussion**
- **The Best Exercise Outcome Is a Gap You Find Before the Emergency Does.**
- **Identify where assistance may be needed from the AE, ODP, emergency management, other providers, county resources, Commonwealth agencies, CISA or other partners.**

The Extended Cyberattack



Administrative & Payment Disruption

Scenario

A sophisticated ransomware attack disrupts critical state and provider systems. HCSIS, billing-related systems, email, electronic records, and other administrative platforms become unavailable. The outage is initially expected to last **72 hours but extends to 14 business days.**

Providers cannot reliably submit claims, access critical records, verify authorizations, communicate through normal channels, or confirm current information for some individuals.

As the outage continues, providers begin reporting payroll concerns, medication-record access problems, staffing difficulties, and uncertainty about authorizations and billing.

Key Discussion Points

Service Continuity

- What services must continue regardless of system availability?
- What information does the provider need immediately to operate safely?
- What paper/manual processes are available and who can authorize them?
- How are critical individual needs identified when electronic records are unavailable?



Key Discussion Points Continued



Financial Continuity

- At what point does an extended outage become a provider financial emergency?
- How will providers maintain payroll, purchase medications, obtain food, and pay essential vendors?
- What mechanisms exist for communicating billing and payment contingencies?

Key Discussion Points Continued

Documentation & Compliance

- What documentation must be maintained manually?
- How will providers reconstruct records after systems return?
- How do providers distinguish between required documentation and information that can be reconstructed later?



Key Discussion Points Continued



Communication

- What happens if normal email and electronic communication are unavailable?
- What is the provider's backup communication tree?
- How are individuals, families, staff, AEs, ODP, and emergency partners kept informed?
- Who has authority to issue operational guidance to staff?

The Extended Cyberattack Hotwash



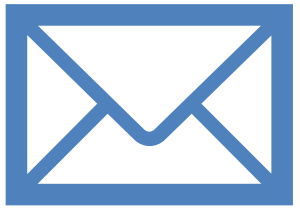
Three Ups – Things that went right.

Three Downs – Things that were challenging.

Questions? Let's talk



- Q&A Session



- Contact Info: danielm@pa.gov