American Hospital Association™
Advancing Health in America

Readiness Advisory

October 29, 2020

Resources for Managing the Risks of Civil Unrest

At A Glance

As the election nears, the news media has reported fears of potential unrest over the outcome of the elections. While federal, state and local government officials have prepared for the possibility of such unrest, to AHA's knowledge, no credible threats or information of such activity have come to light at this time.

Whether it's the possibility of protests, demonstrations, or untoward actions by large groups, which can result in injuries or casualties along with disruptions to business as usual, our field's collective responsibility is to maintain our focus on readiness and preparedness. This is the mission of hospitals and health systems, which are cornerstones of their communities. That is why the AHA stands ready to provide hospitals and health systems with technical assistance to weather challenging events and maintain their ability to continue providing lifesaving-care to their patients and community.

Key Takeaways

Hospitals and health systems should:

- Review their emergency readiness plans and consider setting up a command center.
- Review this advisory and HHS resources about protecting communities during civil unrest.
- Reach out to local community officials and law enforcement to coordinate.
- Review security protocols and remain vigilant about cyber threats.

This advisory pulls together resources and strategies for creating care capacity, keeping people safe, ensuring safe transport, keeping information safe, monitoring social media and mitigating community shutdowns. It also provides additional resources and emergency contacts.

What You Can Do

Please share this advisory with your leadership team, including your emergency readiness and communications teams. Consider the following resources to aid your staff and facilities' preparations for the potential of civil unrest.

Further Questions

Contact John Riggi at jriggi@aha.org, AHA's senior advisor for cybersecurity and risk, or Roslyne Schulman, AHA's director for policy development, at rschulman@aha.org.

Resources for Hospital Emergency Preparedness

CREATING CARE CAPACITY
Plan on activating your facility's emergency plan and standing up an emergency operations center (EOC) in preparation. Ensure that your central command office is set up, phone lines and communication tools are tested, appropriate unit supplies are available, and available emergency decontamination supplies are confirmed.

[See Planning for the Worst: How Hospitals Prepared for the Stanley Cup Riot in Vancouver]

KEEPING PEOPLE SAFE
Review security and access protocols for your physical sites to ensure adequate security rounds and staffing for internal and external areas as well as appropriate processes for employees' and visitors' signing in and identification. If you rely on off-duty police for security, anticipate that they may be called into service for community policing and therefore unavailable for your facilities' use.

[*See this excerpt from Leading Healthcare Risk Management, a publication from AHA's affiliate the American Society for Health Care Risk Management, for a more comprehensive list of considerations of safety and security events, risk assessment, response planning and preparation.]*

ENSURING SAFE TRANSPORT
Coordinate with community officials to determine where hot spots of unease and unrest are occurring; share this information with your staff so they might adjust their commutes accordingly. Adjust staff hours to arrive or depart earlier or later to avoid periods of planned protest. In the event of a curfew, confirm with community officials whether badges are sufficient forms of identification for your essential personnel, or if letters of transit are required for employees whose shifts begin or end during curfew hours.

Review parking plans to ensure staff and visitor vehicles are parked in areas close to facilities and able to be monitored or guarded against vandalism. In case conditions may not allow staff to travel safely home, make overnight accommodations for staff for their safety.

[See A Long Night in the Emergency Department during the Baltimore, Maryland (USA) Riots.]

KEEPING INFORMATION SAFE
When organizations are occupied with addressing physical disruptions and threats, cyber adversaries can take advantage of these distraction. Foreign agents, criminal organizations and ideologically motivated hacktivists may launch attacks to disseminate disinformation to foment unrest, steal sensitive data or conduct ransomware attacks.

Preparedness is key. Incident response plans should be readied for activation. Resources are available from the National Institute of Standards and Technology. It is also important that your cybersecurity teams rely on trusted sources, such as the Cybersecurity and Infrastructure Security Agency, for the latest cyber threat intelligence and to identify the latest cyber vulnerabilities.

Threat intelligence related to various hazards also may obtained from the FBI-sponsored InfraGard site and the Health-Information Sharing and Analysis Center. **Patching medical device cyber vulnerabilities is critical to protect patient care and safety.** FDA guidance and resources can be found here; additionally, the Health Sector Coordinating Council (HSCC) recently published a joint security plan for medical devices and health IT.

Further cybersecurity related information and resources may be found on AHA's cybersecurity site.

MONITORING SOCIAL MEDIA

Review social feeds closely for mentions of your facility, whether as potential targets for protests or for employee posts that draw your facility into unwanted conversations. Because groups may attempt to spread disinformation via social media platforms and phony news outlets, remind staff of the threat of disinformation; encourage them to rely on trusted media sources for their information.

[See this excerpt from the Human Capital Playbook, a publication from the American Society for Health Care Risk Management, for more information on employee-related social media considerations.]

MITIGATING COMMUNITY SHUTDOWNS

Local resources might be stretched thin to address community incidents. Police, fire and other first responders may experience higher call volumes. Other community services, ranging from retail pharmacies and grocery stores to urgent care centers and social services, may be closed or inaccessible. Therefore, your organization may see an influx of individuals in need of first aid, food, shelter or other needs they would otherwise seek elsewhere.

ADDITIONAL RESOURCES

The Department of Health and Human Services' Office of the Assistant Secretary for Preparedness and Response (ASPR) earlier this summer shared resources for protecting community hospitals and providing care during civil unrest. The AHA highlighted this resource for members on June 5.

Collected by ASPR's Technical Resources, Assistance Center, and Information Exchange, the resources cover planning for civil unrest and lessons learned; symptoms and treatment strategies for exposure to riot control tools (e.g., pepper spray, tear gas and rubber bullets); and hospital lockdown procedures for various types of events.

AHA has compiled resources for supporting victims and communities of mass violence incidents, including guidance specific to the COVID-19 environment.

EMERGENCY CONTACTS
For immediate assistance, pressing emergencies, violence or physical threats, hospital staff should call **9-1-1** and share the nature of the emergency, location and assistance required. The dispatcher will ask for any identifying information on witnesses and possible suspects.

For cyber related threats:
FBI:
https://www.fbi.gov/contact-us/field-offices
www.ic3.gov
24/7 Cyber Watch Center 855-292-3937

- Lead agency for investigation and attribution of national security and criminal cyber threats.

Department of Homeland Security Cybersecurity and Infrastructure Security Agency:
https://us-cert.cisa.gov/forms/report

- Maintains responsibility for prevention of cyberattacks and assistance in recovery from a cyberattack targeting critical infrastructure, including health care.

Secret Service:
https://www.secretservice.gov/contact/field-offices

- Investigative authority for cyber criminal threats and related financial fraud, with some overlapping jurisdiction on criminal cyber threats with the FBI.

These federal agencies work closely with AHA and have prioritized hospitals in their cyber incidence response.