Emergency Management and Response - Information Sharing and Analysis Center (EMR-ISAC)

The InfoGram

Volume 20 — Issue 19 | May 7, 2020

Guidance for First Responder Interactions with COVID-19 Patients

The Federal Health Resilience Task Force just released Guidance for First Responder Interactions with Suspected/Confirmed COVID-19 Patients.

The guidance includes a two-page EMS Patient Contact Algorithm, a flowchart detailing recommended best practices starting with first arrival at the scene. Guidance stresses the importance of exposure management regardless of the type of incident.

The Federal Health Resilience Task Force is working to develop comprehensive COVID-19 management strategies for the healthcare system. The task force previously released:

- Epidemiology for COVID-19 Emergency Medical Service Providers: What You Need to Know.
- Alternate Care Site Toolkit.
- COVID-19: Considerations, Strategies, and Resources for Emergency Medical Services Crisis Standards of Care.
- Managing Patient and Family Distress Associated with COVID-19 in the Prehospital Care Setting - Tips for Emergency Medical Services Personnel.
- COVID-19 Behavioral Health Resources for First Responders.

You can find more guidance and information from the task force on the EMS.gov website.

(Source: Federal Healthcare Resilience Task Force)

Drug use, overdose, naloxone use soars as people get stuck at home

Many states and municipalities report higher than normal overdose cases, likely due to the stay-at-home orders imposed over the past few months.

What's more, because of social distancing guidelines many people are getting high alone. If someone does overdose it is less likely anyone will be there to find them and call for help or administer nalaxone.

Social isolation is a component in relapse among drug users under normal circumstances. With fewer healthy outlets and the inability to socialize with friends or family, people with drug problems find themselves fighting an uphill battle. Nalaxone use is up sharply in many locations.

In addition to the expected opioids, opioid analogs and other street drugs, areas of Canada report an increase in both isotonitazene and etizolam. In one case, an overdose victim needed six doses of nalaxone to save their life.

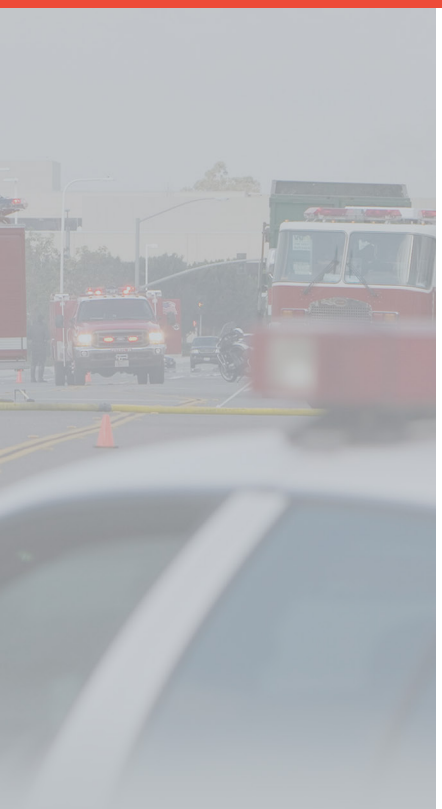
Health departments and first responders around the country should evaluate their supply of nalaxone drugs at this time. It is unknown how long stay-at-home orders may continue in different parts of the country or if and when we will need to reimpose them in the future.

Highlights

U.S. Fire Administration

The U.S. Fire Administration operates the Emergency Management and Response – Information Sharing and Analysis Center (EMR-ISAC).

For information regarding the EMR-ISAC visit www.usfa.dhs.gov/emr-isac or contact the EMR-ISAC office at: (301) 447-1325 and/or emr-isac@fema.dhs.gov.



It is also a good idea to review signs and symptoms of overdose so you can recognize it if you or members of your team get exposed at an incident or scene.

The possibly good news is COVID-19 may have disrupted the supply of fentanyl out of Mexico due to supply chain disruption from China. As Wuhan shut down, shipments of chemical precursors slowed as did production in Mexico. This has driven the price of fentanyl up, putting it out of reach for many people.

(Source: Various)

ICE launches website to combat COVID-19 fraud, counterfeit products

The United States Immigration and Customs Enforcement's Homeland Security Investigations (HSI) unveiled the new webpage Operation Stolen Promise to fight the ever-growing criminal activity surrounding COVID-19: fraud campaigns, counterfeit items such as PPE and test kits, and scams concerning stimulus checks or other financial relief.

All first responders should be especially aware of counterfeit items related to response and safety. Fake PPE have the potential to endanger personnel while unapproved pharmaceuticals and test kits may risk the lives of the people you serve. All these things have the potential to disrupt response operations in some way.

Law enforcement needs to count HSI and Operation Stolen Promise as a resource when educating the public on fraud, scams and cyberattacks related to COVID-19. HSI has an educational fact sheet available you can link to or distribute. There is also a public-facing email address to report suspected fraud: covid19fraud@dhs.gov.

HSI is dividing its efforts between four methods: Partnership, Investigation, Disruption and Education. In addition to educating the public on the signs of fraud and counterfeit items, you and your department can help HSI by reporting fraud and working with them through existing partnerships.

(Source: ICE HSI)

State of 911 Webinar: GIS data and COVID-19, translating text-to-911

The next State of 911 Webinar is scheduled for Tuesday, May 12, 2020, from 12-1 p.m. Eastern. It will cover lessons learned in two key topic areas: using GIS data in the era of COVID-19 and approaches for translating non-English requests for help through Text-to-911. Registration is required.

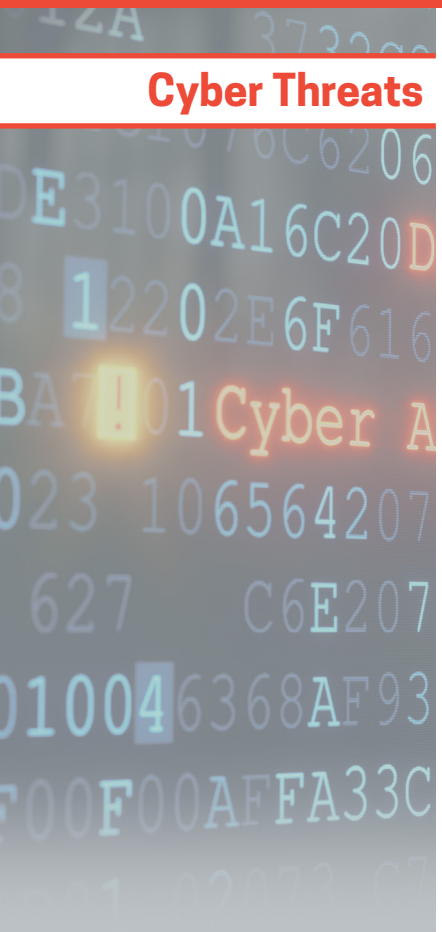
As the 911 industry works to improve GIS data for the transition to NG911, other benefits include accurate COVID-19-related data. Join the Maryland Department of Information Technology Geographic Information Office, the Maryland Emergency Management Agency and the Maryland Department of Health to learn how they strive to maintain and improve access to accurate and timely data related to COVID-19 in Maryland.

The second topic addresses challenges individuals with limited English proficiency may experience in emergency situations when communicating with public safety officials. As Text-to-911 becomes common across the nation, public safety telecommunicators will receive more non-English texts, resulting in increased needs for translation services.

After you register, you will be sent the connection information. All past webinar recordings are available on the 911.gov website.

(Source: 911.gov)

Cyber Threats



Microsoft Teams vulnerability allowed takeover of accounts

Microsoft has fixed a subdomain takeover vulnerability in its collaboration platform Microsoft Teams that could have allowed an inside attacker to weaponize a single GIF image and use it to pilfer data from targeted systems and take over all of an organization's Teams accounts.

The attack involved tricking a victim into viewing a malicious GIF image for it to work. Microsoft neutralized the threat last Monday, updating misconfigured DNS records, after researchers reported the vulnerability on March 23.

(Source: Threatpost)

Cyber authorities warn hackers are after COVID-19 treatment data

Advanced persistent threat (APT) groups appear to be after intellectual property and research that could aid nation-states in their attempts to treat the coronavirus pandemic, according to an alert jointly issued by the Cybersecurity and Infrastructure Security Agency and the United Kingdom's National Cyber Security Centre.

APTs are typically associated with nation-states because of the level of sophistication and resources they are able to put into their hacking campaigns.

This alert does not name any particular nation-states, but United Kingdom authorities reportedly suspect Russia, Iran and China are responsible for a recent uptick – yet unsuccessful – in attacks.

(Source: Nextgov)

Cybercrime reporting tips sheet, Unified Message from US government

The United States government has several ways your agency, department or business and the general public can report cybercrime. The following documents alist steps to take if you think you've been a victim of cybercrime as well as specific agencies to contact for different types of cybercrime or complaints.

- The one-page Reporting a Cybercrime Complaint Tip Card is a great resource to post in an office, send to employees or make available to the jurisdiction you serve.
- Cyber Incident Report: A Unified Message for Reporting to the Federal Government covers the same information in more detail.

(Source: Various)

Cybersecurity and Health Sector Webinar

Countries around the world report a rise in disruptive cyberattacks against the healthcare sector during the COVID-19 pandemic. As medical facilities are strained around the world, these attacks compound the current situation by denying or ransoming critical healthcare services by disabling relevant systems.

Join the Cybersecurity and Health Sector Webinar on Thursday, May 14, 2020, from 10-11 a.m. Eastern. This session will focus on public-private cyber strategies to promote resilience, recovery, and common defense.

Registration is required for this event, after which you will receive connection details.

(Source: U.S. Chamber of Commerce)

Cyber Information and Incident Assistance Links

MS-ISAC
SOC@cisecurity.org
1-866-787-4722

IdentityTheft.gov

IC3

Cybercrime Support Network

General Information Links

FTC scam list

CISA alerts

Law Enforcement Cyber Center

TLP Information