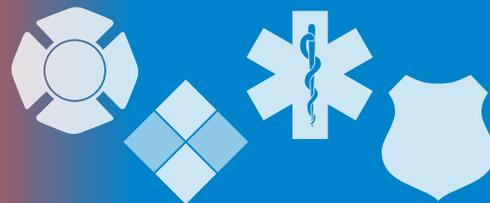


The InfoGram



Volume 20 — Issue 16 | April 17, 2020

PPE Preservation Best Practices: reduce, reuse, repurpose

The Federal Emergency Management Agency (FEMA) just released "[Coronavirus \(COVID-19\) Pandemic: Personal Protective Equipment Preservation Best Practices](#)," guidance to assist healthcare workers and first responders manage critical shortages of PPE. The guidance recommends healthcare facilities start implementing PPE contingency strategies now to avoid future PPE shortages.

Best practices for maximizing PPE use:

- Reducing PPE usage rates through changes in operations and procedure. Examples of this include using tele-consultation to see patients and using other forms of barrier control where possible.
- Reuse PPE through use optimization and proper decontamination. Be sure to follow decontamination procedures outlined by the Centers for Disease Control and Prevention (CDC) and the Food and Drug Administration.
- Repurpose other forms of PPE and seek alternative supplies or suppliers. This might include using different types of masks and asking for donations from the general public or from businesses not currently operating, such as dentists offices.

FEMA recommends affected agencies form a team to review existing procedures and identify opportunities to utilize the strategies listed above.

(Source: [FEMA](#))

Letter of guidance, appreciation to emergency managers from FEMA

FEMA Administrator Pete Gaynor just released a [letter to the nation's emergency managers](#) thanking you for your hard work during this crisis and discussing the successes and lessons learned from the first 30 days of the "Whole-of-America" pandemic response.

In the letter, he specifically mentions the PPE supply, use and reuse issue, and stresses getting PPE to the people on the front lines – medical staff, first responders and those in jobs critical to keeping our infrastructure operational – is and has been the top priority.

Administrator Gaynor also highlights the emergency manager's role in:

- Encouraging facilities to use the National Health and Safety Network (NHSN) tracking system to collect and report data to responding federal agencies.
- Determining when peak may occur in your local jurisdiction so you can better manage resources and make requests to manage shortfalls.
- Developing a flexible plan to utilize federal medical staff, if needed.
- Strengthening the supply chain, flattening the curve and busting myths when possible.

Emergency managers and other responders with questions can contact the FEMA



Highlights

PPE Preservation Best Practices: reduce, reuse, repurpose

Letter of guidance, appreciation to emergency managers from FEMA

911 guidance for pandemic response

Webinar: EMS Patient Care and Operations

Cyber Threats

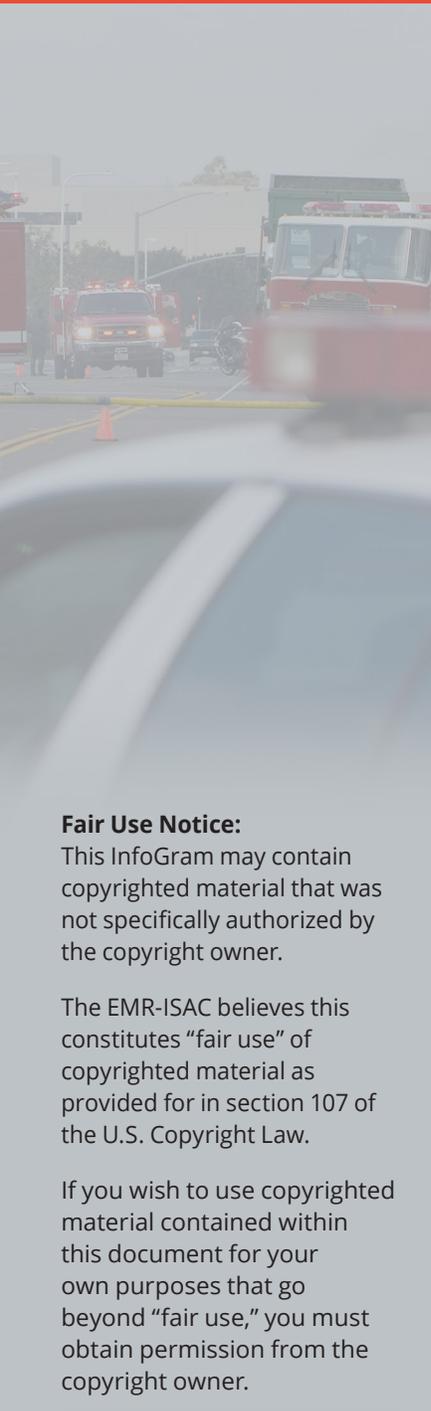


U.S. Fire Administration

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.

[Subscribe here](#)



offices for [Congressional Affairs](#), [Intergovernmental Affairs](#), [Tribal Affairs](#) or [Private Sector Engagement](#).

(Source: [FEMA](#))

911 guidance for pandemic response

This week is [National Public Safety Telecommunicators Week](#) which focuses on the important job our 911 operators do throughout the year. This year it happens to fall during a serious national emergency. Some 911 officials suggest [this crisis may permanently change how PSAPs operate](#) by taking on duties they never would have imagined just weeks ago.

The National Emergency Numbers Association (NENA) released [9-1-1 & COVID-19: A Report on PSAPs During the Pandemic](#), showing the early impact to PSAPs and 911. Based on survey results of 500 PSAPs, the report looks at call volume, safety measures for staffing, staff's stress and anxiety, impact on technology and more. The data points are worth considering when adjusting plans for future emergencies and creating opportunities for growth and change as part of the greater emergency response team.

Several agencies have recently published new guidance to support 911 response to COVID-19:

- ❶ [Public Safety Answering Point \(PSAP\)/Emergency Communications Centers \(ECC\) Call Screening](#) from the Healthcare Resilience Task Force lists updated guidance for initial call screening of potential COVID-19 cases. Asking about recent travel is no longer recommended.
- ❷ [911 and Emergency Medical Services \(EMS\) Algorithms](#), just released today by the Healthcare Resilience Task Force, lists step-by-step procedures that should be considered as part of the 911 center's screening process.
- ❸ Though it specifies influenza, the information in [Preparing for Pandemic Influenza: Recommendations for Protocol Development for 911 Personnel and Public Safety Answering Points](#) is applicable to this pandemic as well. It can be used as a guide to develop better practices for future pandemic emergencies.
- ❹ The Association of Public-Safety Communications Officials (APCO) International's [COVID-19 page](#) links to two 911-related webinar recordings and a discussion forum for members to share information and advice.

(Sources: Various)

Webinar: EMS Patient Care and Operations

Join EMS providers from across the country to discuss challenges faced in the COVID-19 response and what can be done to enhance patient care and emergency operations.

The U.S. Department of Health and Human Services Assistant Secretary for Preparedness and Response (ASPR) is co-hosting the webinar "EMS: Patient Care and Operations" on Monday, April 20, 2020, from 12-1 p.m. Eastern. [Click here for registration and connection information](#).

This webinar is part of the COVID-19 Clinical Rounds series. Those interested may [view recordings and slides of past webinars in this series](#).

(Source: [ASPR](#))

Fair Use Notice:

This InfoGram may contain copyrighted material that was not specifically authorized by the copyright owner.

The EMR-ISAC believes this constitutes "fair use" of copyrighted material as provided for in section 107 of the U.S. Copyright Law.

If you wish to use copyrighted material contained within this document for your own purposes that go beyond "fair use," you must obtain permission from the copyright owner.

Disclaimer of Endorsement:

The appearance of external hyperlinks does not constitute endorsement of the linked websites or the information, products or services contained therein. Reference to any specific commercial products, process or service by trade name, trademark, manufacturer or otherwise, does not necessarily constitute or imply its endorsement, recommendation or favoring by the EMR-ISAC or the U.S. government.

Cyber Threats

U.S. Government warns of North Korea cyber threat

Several federal agencies released an advisory this week detailing the cyber threat posed by North Korea. The advisory also covers recommendations to mitigate the threat.

North Korea's malicious cyber activities threaten the United States and the broader international community and, in particular, pose a significant threat to the integrity. North Korea has increasingly relied on illicit activities - including cybercrime - to generate revenue for its weapons of mass destruction and ballistic missile programs.

In particular, the United States is deeply concerned about North Korea's malicious cyber activities. North Korea has the capability to conduct disruptive or destructive cyber activities and uses cyber capabilities to steal from financial institutions.

It is vital for the international community, network defenders, and the public to stay vigilant and to work together to mitigate the cyber threat posed by North Korea.

(Source: [US-CERT](#))

Dark patterns: social engineering

A dark pattern is a type of social engineering technique whereby businesses or other organizations use crafty user interface/user experience (UI/UX) designs to manipulate users into making unintended choices.

Dark patterns are often used to charge unwitting customers money, maintain a user's attention, harvest personal data, gain or retain subscribers, and display advertisements. One example is how social media platforms use dark patterns to trick users into uploading their personal contact lists when they first open an account so that the platforms can market themselves to new users and collect additional data.

[See these tips to avoid dark patterns and protect your information.](#)

(Source: [National Capital Region Threat Intelligence Consortium](#))

US, UK officials: state-backed hackers taking advantage of outbreak

American and British cybersecurity officials are warning that state-backed hackers and online criminals are taking advantage of the coronavirus outbreak to further their operations, echoing concerns from digital safety experts.

A joint advisory published on Wednesday by the United States' Cybersecurity and Infrastructure Agency and Britain's National Cyber Security Centre said that while the overall volume of malicious activity does not appear to have changed, hackers of all varieties were leveraging anxiety around the disease outbreak to push people into clicking links and downloading attachments.

The agencies warned that hackers were also exploiting growing demand for work-from-home solutions by passing off their malicious tools as remote collaboration software produced by Zoom and Microsoft. Hackers are also targeting the virtual private networks that are allowing an increasing number of employees to connect to their offices, the agencies said.

(Source: [Reuters](#))

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](#)