



Highlights:

Using Secure Incident Response Data in the Field

EMS Week Recognizes those Always in Service

Healthcare Public Health Cybersecurity

Webinar: Scene Safety in EMS Operations

Disclaimer of Endorsement:

The EMR-ISAC does not endorse the organizations sponsoring linked websites, and does not endorse the views they express or the products/services they offer.



The U.S. Fire Administration maintains 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.

The InfoGram

Volume 17 – Issue 21

May 25, 2017

Using Secure Incident Response Data in the Field

Events at venues and stadiums are a prime target for a terrorist attack due to the large number of people, as we have seen in Europe recently. This year's Super Bowl brought a million people to the Houston area for the big game, and [Houston's public safety agencies had "datacasting" technology helping them monitor the events](#) for any sign of a threat to the crowds and city.

Datacasting uses the [public television broadcast network](#) to share videos, images, maps and text from a variety of old and new technology such as stationary cameras and mobile devices. It allows personnel close to an accident scene, for example, to stream real-time video back to an emergency operations center so those in charge can determine what level of response is necessary.

One benefit of datacasting is the ability to send and receive encrypted content even in areas with degraded or nonexistent wireless signals, providing communications support where wireless access may be poor at best.

This is the fifth time Houston used datacasting as a tool in its emergency operations. Previous uses include other sporting events, a presidential political debate, and during [response to the serious floods in 2016](#).

Datacasting was developed by the Department of Homeland Security Science and Technology Directorate's First Responders Group (FRG). Agencies interested in more information can visit the [Voice, Video, and Data for Public Safety](#) program page or contact the FRG at First.Responder@hq.dhs.gov.

(Source: [DHS S&T First Responders Group](#))

EMS Week Recognizes Those Always in Service

This is EMS Week, May 21-27, 2017, and the theme is "[EMS Strong – Always in Service](#)." National EMS Week is an important opportunity for fire and EMS departments to highlight their call to care through events such as open houses, demonstrations, educational presentations and media programs.

EMS services are often taken for granted not only by the public but by those responsible for budget and resource allocation. Because of this, EMS departments are often not adequately funded or supported in communities. This is especially true for volunteer departments, where they have the added struggle of finding people willing and able to sign on for hours of rigorous training and testing before even beginning a shift.

The InfoGram is distributed weekly to provide members of the Emergency Services Sector with information concerning the protection of their critical infrastructures.

EMS Week is a good time to begin outreach programs, creating a more educated public and developing inroads with administration and elected officials to ensure departmental needs are met. Make plans to continue outreach through the year:

Offer ride-along opportunities to local officials or members of the media.

- [Teach CPR in an innovative way.](#)
- Start a “[Second Chance](#)” annual event.
- Visit the schools – yes, even high schools or local colleges – to teach about EMS as a service and a career or volunteer opportunity.

More information on EMS programs, outreach and activities can be found on the [U.S. Fire Administration website](#).

(Source: [EMS Strong](#))

Healthcare Public Health Cybersecurity Resources

Last week’s ransomware attack was especially hard on some [healthcare organizations overseas](#), and federal agencies here in the United States were quick to issue warnings to be especially watchful for such attacks.

The Health and Public Health portal in the Homeland Security Information Network (HSIN-HPH) has a new online library compiling information on cybersecurity threats facing this sector.

The Health and Public Health Sector Cyber Threat Library includes situational awareness information on cybersecurity from the FBI, Department of Homeland Security, Health and Human Services, the Office of the Director of National Intelligence, National Healthcare Information Sharing and Analysis Center (NH-ISAC), the Multi-State ISAC (MS-ISAC), and others.

Those interested in accessing the library need an active HSIN account and access to the HSIN-HPH portal. Please send access requests to hsinci@dhs.gov. Please see the [DHS website](#) for more information on HSIN, the communities available and how it can serve you.

(Source: [DHS](#))

Webinar: Scene Safety in EMS Operations

Firefighters and EMS personnel must deal with the [potential for assault and violence](#) as part of the job, but it is possible to mitigate that threat to some extent using situational awareness tactics. Practicing good scene safety size-up on every call and maintaining situational awareness during the call can go a long way to ensuring you and your team go home at the end of every shift.

The International Public Safety Association (IPSA) is hosting the “[Is the Scene Safe?](#)” webinar on Wednesday, June 7, 2017, from 1:00 p.m. to 2:00 p.m. Eastern. This is a web-based training for firefighters and EMS workers on how to determine if the scene is safe and to go over things you can even do prior to arrival to ensure safety. Participants will receive a certificate of completion.

Please see the event page for more information on registering.

(Source: [IPSA](#))

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.

DHS and the FBI encourage recipients of this document to report information concerning suspicious or criminal activity to the local [FBI office](#) and also the [State or Major Urban Area Fusion Center](#).

For information specifically affecting the private sector critical infrastructure contact the [National Infrastructure Coordinating Center](#) by phone at 202-282-9201, or by email at nicc@dhs.gov.