EMR-ISAC
Emergency Management & Response-Information Sharing & Analysis Center

# The InfoGram

*Volume 17 – Issue 18* *May 4, 2017*

## Highlights:





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.**

## Interim Guidance: Safe EMS Transport of Children

In March, the National Association of State EMS Officials (NASEMSO) announced the release of "Safe Transport of Children by EMS: Interim Guidance" (PDF, 296 Kb), a recommended set of practices for ambulance transport of children supported by evidence-based standards.

EMS providers and their pediatric patients must rely on ambulance manufacturers to supply sturdy, well-made, and effective restraints and, unlike restraints used in passenger vehicles, there are no required crash-testing standards for these restraints. This may change as funding for such testing is being sought, but for now, NASEMSO issued this interim guidance in an attempt to address the issue. Some recommendations for safely transporting children:

- Develop policies and procedures addressing methods, training, and equipment to secure children in a way to reduce forward motion and possible ejection;
- The primary focus should be to secure the torso, and provide support for the head, neck, and spine of the child;
- Prohibit transporting children unrestrained;
- Only use restraints as they were intended to be used by the manufacturer;
- Consider the manufacturer's recommendations when selecting the appropriate device, dependent on the size and weight of the child.

The guidance is a result of the work of NASEMSO's Safe Transport of Children Ad Hoc Committee, comprised of members from state EMS for Children programs, federal partners, children's hospitals, the Ambulance Manufacturers Division of the NTEA, and the Association of Air Medical Services (AAMS).

*(Source: NASEMSO)*

## "May the 4th" Help You Create Strong Passwords

More commonly known as "Star Wars Day," May 4th is also now designated as "World Password Day" and everyone is reminded to use strong passwords, change them frequently, and update old weak passwords to protect their digital information.

Recent statistics show 90 percent of all passwords can be broken in seconds. People are just not using strong passwords – containing capital and lower case letters, num-

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

bers, and symbols – to secure their information and online identities.

We should create a different strong password for each site, but this can mean dozens of long, hard-to-remember passwords all competing for memory space in our brains. For many people it's just one more thing to manage daily and they don't bother. However, there are numerous reputable password manager apps available for smartphones, many of them free, and other ways to securely keep a list of passwords handy so you don't have to remember them all.

Passwords should be nine or more characters long and have a mix of capitals, lower case, numbers, and symbols. One trick is to pick a random long word you can easily remember (i.e., contingencies) and changing the letters to fit the requirements of the site (i.e., C0nt!ngeNc1e$).

Don't use names of family members or pets, numeral-only passwords, or words you can find in the dictionary or on a map. When you begin upgrading your accounts to strong passwords, start with the most important ones like banking, email, work accounts, and medical sites. Use different strong passwords for sites like social media or shopping as well. If someone gets ahold of one of your passwords, they will try it on every account you have. Unique passwords for every site fixes this.

If you use an electronic-based password manager, vet the program well. Ensure it is a sound program, properly encrypted, and is respected in the industry.

Change your password frequently; consider the fact that your login information may already be compromised and start changing them now. Finally, consider using dual-factor authentication. If your email account is set to send you a pin number by text, the hacker won't be able to access your account.

*(Source: World Password Day)*

## Webinars for Medical Facilities and Healthcare

The Technical Resources, Assistance Center, and Information Exchange (TRACIE) is holding another free offering of the "Highly Pathogenic Infectious Disease Exercise Planning for Frontline Facilities" webinar on Wednesday, May 24th from 2:00 p.m. to 3:00 p.m. Eastern. Space is very limited and they recommend early registration. This webinar will cover the National Ebola Training and Education Center's suite of free, customizable exercise materials; exercise methodology and management; and lessons learned.

A free recording of the February 6th webinar "Communicating During a Crisis: What a Hospital Epidemiologist Needs to Know" is now available courtesy of the Centers for Disease Control and Prevention. This was the first in a series on crisis communication geared toward epidemiologists covering communicating risk, tailoring messages for specific audiences, and communication planning. This webinar was created in collaboration with the Society for Healthcare Epidemiology of America.

Finally, another free recording "Cybersecurity and Healthcare Facilities" is available from TRACIE. This webcast covers cybersecurity issues for healthcare preparedness professionals, lessons learned from recent incidents, planning, and steps the federal government is taking to address cybersecurity.

*(Sources: Various)*



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**.