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

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.**

The InfoGram

Volume 17 – Issue 15 *April 13, 2017*

Managing HIPAA During Disasters, Part 1

During a disaster or mass casualty incident, healthcare staff and public information officers must be able to handle requests for patient information while staying within the Health Insurance Portability and Accountability Act (HIPAA) privacy rules. These rules are in place to protect patient health information (PHI), but they allow disclosure of information in certain circumstances. It is important those involved in disaster response and recovery know these rules.

The Technical Resources, Assistance Center, and Information Exchange (TRACIE) created the six-page fact sheet discussing the various aspects of HIPAA and disasters. "HIPAA and Disasters: What Emergency Professionals Need to Know" (PDF, 162 Kb) defines who is bound by HIPAA, what information is protected, who may disclose PHI, and when that can happen. It also discusses when a HIPAA-covered entity can disclose PHI to law enforcement, and how HIPAA rules apply to foreign nationals.

Health and Human Services (HHS) offer more resources covering this issue, including a decision tool, how HIPAA waivers work and when they are enacted, and HIPAA disclosure checklists. Next week, we will cover handling HIPAA breaches in disasters.

(Source: HHS)

P25 CAP Program for Radio Interoperability

First responders' struggles with interoperable communications have hampered response for decades, costing communities time, money, and most importantly, lives. The most notable example is September 11th, but incompatible radio technologies regularly compromise routine emergency operations across the country.

Project 25 (P25) is a suite of standards ensuring digital two-way land mobile radio interoperability. P25 Compliance Assessment Program (CAP) is the formal, independent testing process for P25 compliance and the recommended starting point for public safety to acquire radio technology guaranteed to be interoperable. P25 CAP maintains an approved publicly available list of independently tested equipment complying with the P25 Standard. Communications systems go through rigorous testing to ensure interoperability, and as technology evolves so do the standards and testing.

The Department of Homeland Security (DHS) recently announced changes to address encrypted radio equipment, which was previously not part of the P25 compliance testing. Encrypted communications are becoming more mainstream, and using non-standard encryption technology intensifies the existing interoperability problems.

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

P25 Cap is a partnership of the DHS Office of Interoperability and Compatibility, industry, and the emergency response community. For more detailed information on the P25 program, please see the video, fact sheet, and FAQ section of the P25 website.

(Source: P25)

The Dallas Siren System "Hack" That Wasn't

Dallas, Texas, has an outdoor warning siren system to alert people to get inside when dangerous weather is closing in. Late Friday night, someone triggered all 156 sirens across the city to go off at the same time, and was able to keep them going for an hour and a half despite workers shutting them off. 9-1-1 was inundated with calls, city dwellers were frightened and confused, and city workers literally had to unplug the system to shut it down.

Initially believed to be another successful hacking attack, officials eventually found the real cause: the system is radio-controlled and activated, and someone sent tones to receivers attached to the 156 sirens, turning them on at the same time. The culprit was traced to the Dallas area and municipal and federal agencies are investigating.

It is unknown how Dallas secured their system, but some theorize if any encryption was in effect it was likely low-level and more easily breached. The city has since installed more security and encryption and are looking to purchase a new system. It is also unknown if this was done "for fun" or if there was a more nefarious reason. For many criminal elements, a timed disruption like this would be quite beneficial.

Dallas' mayor has called this "yet another serious example of the need for us to upgrade and better safeguard our city's technology infrastructure," something other towns and cities with such siren systems should also be thinking about. The domino effect of this incident to Dallas emergency services in terms of time, money, and resources spent is unknown. Other communities should take notice of this incident and bolster security if they use similar systems.

(Source: Dallas News)

National Information Exchange Model

The National Information Exchange Model (NIEM), created as a joint effort between the Departments of Justice and Homeland Security, is working on an upcoming Major Release which will update NIEM's core and technical architecture. It also includes updates to existing domains, including Emergency Management, Justice, Military Operations, Surface Transportation, Biometrics, and Human Services.

NIEM requests public review and comment on NIEM 4.0 beta1. Please refer to the full NIEM 4.0 beta1 release information and the Naming and Design Rules. All comments can go to niem-comments@lists.gatech.edu through April 21, 2017. Those interested in NIEM can also connect to it via Twitter (@NIEMconnects) and LinkedIn.

NIEM is a standard vocabulary enabling different public and private organizations to exchange information more efficiently, especially when using computer systems. For example, if we use the word "automobile" in an online form and another organizations uses "car" in its form, the information would not sync. It may seem minor, but changing how organizations talk to each other by using NIEM has saved millions of dollars and some workflows were shortened from nearly a year to just days.

(Source: NIEM)

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**.