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

The InfoGram

Volume 19 — Issue 1 | January 31, 2019

A Case Study of the Las Vegas Mass Shooting: hospital response

The Nevada Hospital Association released a case study on the medical response to the Las Vegas, Nevada, Harvest Festival shooting. The purpose of this case study is to provide hospitals and public health agencies points of discussion to further their emergency management and mass casualty planning.

"A Day Like No Other: A Case Study of the Las Vegas Mass Shooting" covers an incredible amount of detail on several topics, reviewing triage, staffing, safety and security, communications, surge plans, mortuary care, and mental health and wellness. Any hospital or EMS agency writing or reworking its mass casualty response plan should review this case study. These are a few take-aways from this case study:

- Injured and deceased people were spread over four square miles around the venue, a very large area for EMS to manage.
- The majority of injured (approximately 800) self-transported, using phone mapping apps to find the *closest* hospital. This should be a planning consideration for events and venues as well as hospitals.
- Hospitals had no notice of the shooting before the injured started arriving.
- The influx of families and friends - and the issues they created - were not planned for. A Family Assistance Center wasn't established until the next day.
- Infection control and contamination was a serious concern due to the amount of blood being spread everywhere. Environmental cleaning was continuous. Ensure you have enough staff and supplies to handle such an incident.
- Hospitals interpreted the Health Insurance Portability and Accountability Act (HIPAA) differently, creating confusion. Review HIPAA policy with a mass casualty incident in mind.
- One hospital used a military-type triage system that worked quite well; however, triage was problematic at best in most locations.

One added problem was that the festival used Radio Frequency Identification Device (RFID) armbands containing ticket and credit card information, and many attendees did not carry identification. This increased confusion as hospitals could not tell anyone, law enforcement or family members, who they were treating because they didn't know.

(Source: Nevada Hospital Association)

Medical mass casualty management checklists

There are a number of checklists, tools, and resource pages available to hospitals and medical staff for managing a mass casualty incident. We have compiled a list here that should be of assistance.

- Select Mass Violence Resources – Technical Resources, Assistance Center, Information Exchange (TRACIE), Department of Health and Human Services.

Highlights

A Case Study of the Las Vegas Mass Shooting: hospital response

Medical mass casualty management checklists

Doxxing: an online threat to your privacy and safety

U.S. Fire Administration

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

- Operating Room Procedures for Mass Casualties (PDF, 68 Kb) – by the American Society of Anesthesiologists.
- Mass Casualty Disaster Plan Checklist (PDF, 84 Kb) – from the Association for Professionals in Infection Control and Epidemiology, Inc.
- Operational Templates and Guidance for EMS Mass Incident Deployment (PDF, 1.61 Mb) – U.S. Fire Administration.
- Mass Casualty Management Systems (PDF, 2.89 Kb) – World Health Organization.
- Hospital Emergency Response Training for Mass Casualty Incidents – Center for Domestic Preparedness (CDP). The CDP has more training available on this topic.
- Incident Planning Guide: Mass Casualty Incident (PDF, 143 Kb) – California Emergency Medical Services Authority.

(Source: Various)

Doxxing: an online threat to your privacy and safety

Doxxing is sharing someone's private and personally identifiable information online to cause them harm. Almost everyone has data online and is at risk, but first responders and especially law enforcement officers are targets of interest.

Many doxxing cases involving public servants or politicians are a form of retaliation or "punishment" triggered by a highly politicized incident or circumstance, such as an officer-involved shooting or unpopular legislation. Some people have had their families threatened, and doxxing can lead to swatting attacks.

Perpetrators gather information in a variety of ways: accessing social media profiles, simple internet searches, online directories, hacking and social engineering. By utilizing a variety of methods, someone can potentially put together a fairly detailed picture of you, your family and your lifestyle.

How you manage your personal information goes a long way toward keeping you safe. The following tips can assist:

- Think carefully before you post anything online.
- Update your software to minimize vulnerabilities.
- Use a different email address and password for each online account you have.
- Search your name, email address and usernames online.
- Use alerts to monitor personal information posted online.
- Tighten social media security settings and delete old social media and email accounts you no longer use.
- Turn off geotagged when posting photos.

(Source: Officer.com)

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.**

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.