The Future Technologies that will Define Disaster Medicine

Alexander Hart MD[1,2], Attila Hertelendy PhD[1,3]
1. Beth Israel Deaconess Medical Center Disaster Medicine Fellowship, Boston, USA
2. Department of Emergency Medicine, Hartford Hospital, Hartford, USA
3. Department of Information Systems and Business Analytics, College of Business, Florida International University, Miami, USA

Introduction: Advances in technology can drastically improve the ability of providers to care for survivors of a disaster. Research into new applications of technology in the Disaster Medicine space, and dissemination of new technological achievements are vital to saving lives. This presentation discusses several recently proven technologies in the field of disaster medicine which deserve further dissemination, as well as promising technologies currently being studied.
Method: An overview of the current uses and upcoming research on several technologies will be definitive in future disaster responses.
Results: Unmanned Aerial Vehicles (UAVs) and Telemedicine have been well studied and are proven game changers in field disaster response. Artificial intelligence continues to be studied and aid real-time, strategic and tactical decision making in the field. Virtual reality simulation has now advanced to be a feasible, cost effective and effective method of training disaster responders as well as for training the lay public in disaster risk reduction. Artificial Intelligence is also being studied for uses in the hospital and in all forms of Emergency Management, and is likely to be intricately tied to the future of the field.
Conclusion: As new technologies are developed, it is important for Disaster medicine practitioners to consider how they can be applied to the field. Advocating for applying new technologies to disaster medicine, and for dissemination of proven technologies is a vital part of advancing the field of disaster preparedness and response.

Prehosp. Disaster Med. 2023;38(Suppl. S1):s89
doi:10.1017/S1049023X23002534

Cyberthreats and Healthcare

Derrick Tin MD[1], Ryan Hata MD[1], Richard Staynings[2], Fredrik Granholm MD[3], Gregory Ciottone MD[1]
1. BIDMC/ Harvard Medical School, Cambridge, USA
2. University of Denver, Denver, USA
3. Swedish Air Ambulance, Mora, Sweden

Introduction: Cyberattacks against healthcare have been growing at an alarming rate globally targeting the theft of clinical research intellectual property, personally identifiable information, and personal health information. Recent studies have also shown a concerning correlation between cyberattacks and patient morbidity and mortality rates. Many top security experts consider cyberattacks a top national security concern.This paper is a descriptive analysis of healthcare-related breaches in the United States in the past decade and an analysis of cybersecurity threats that are currently facing the industry.
Method: Breach reports of unsecured protected health information affecting 500 or more individuals in the US are publicly accessible through the U.S. Department of Health and Human Services Office for Civil Rights portal. The database was downloaded and searched for all reported breaches occurring between January 1, 2011 - December 31, 2021. Breaches were subdivided by states, dates, location, entity type, and individuals affected.
Results: Of the 3,822 PHI breaches recorded, 1,593 (41.7%) were hacking/IT related, 1,055 (27.6%) were listed as unknown, 819 (21.4%) were theft related, 194 (5.1%) were loss related, 97 (2.5%) were related to improper disposal and 64 (1.7%) were listed as "others."

Breaches occurred within the main categories as follows: network server (957 [25%]), email (877 [23%]), paper/films (665 [17%]), other (454 [12%]), laptop (341 [9%]), desktop (309 [8%]), and electronic medical records (220 [6%]).
Conclusion: A total of 3,822 breaches affecting 283,335,803 people in the United States were recorded from January 1, 2011 to December 31, 2021.

The most reported breaches were from healthcare providers with 2,827 (75.1%) events, followed by health plans (500 [13.1%]), business associates (480 [12.6%]) and healthcare clearinghouses (10 [0.3%]). 4 (0.1%) breaches were from unknown sources.

This report may help healthcare providers understand the extent of the issue and mitigate some of the associated risks.

Prehosp. Disaster Med. 2023;38(Suppl. S1):s89
doi:10.1017/S1049023X23002546

Deploying the Red Cross Red Crescent Health Information System (RCHIS) into a Type-One Fixed EMT: How the Use of a Custom Built Application for Electronic Medical Records and Data Reporting Improves Patient Care and Mandatory Reporting.

Lauren Clarke[1], Felix Holl[2,3], Thomas Raffort[1], Elvire Serres[1]
1. International Federation of the Red Cross and Red Crescent, Geneva, Switzerland
2. DigiHealth Institute, Neu-Ulm University of Applied Sciences, Neu-Ulm, Germany
3. German Red Cross, Berlin, Germany

Introduction: RCHIS is an Electronic Medical Record (EMR) and Health Information System (HIS) that has been purpose-built for use by Red Cross Red Crescent (RCRC) Emergency Response Units (ERUs), which are the equivalent of Type 1 (fixed and mobile) and Type 2 facilities in the Emergency Medical Teams (EMT) classification.
Method: A three day in-person super user training was held with 13 participants: 9 first aid volunteers, 2 nurses and 2