SPECIAL REPORT

Secure Scalable Disaster Electronic Medical Record and Tracking System

Gerard DeMers, DO, DHSc, MPH;[1] Christopher Kahn, MD, MPH;[1] Per Johansson;[2] Colleen Buono, MD;[1] Octav Chipara, PhD;[2] William Griswold, PhD;[2] Theodore Chan, MD[1]

1. University of California, San Diego Health System, UCSD EM Department, San Diego, California USA
2. University of California, California Institute for Telecommunications and Information Technology, La Jolla, California USA

Correspondence:
Gerard DeMers, DO, DHSc, MPH
University of California, San Diego Health System
UCSD EM Department
200 W. Arbor Street
San Diego, California 92103 USA
E-mail: gdemers@ucsd.edu

Conflicts of interest and funding: The authors report no conflicts of interest. This work was supported in part by NIH/NLM grant numbers N01-LM-3-3511 and R01-LM009522.

Keywords: disaster; electronic medical record; mass casualty incident; triage

Abbreviations:
IEEE 802.11: a set of standards for implementing wireless local area network (WLAN) computer communication
EMR: electronic medical record
MCI: mass-casualty incident
EMS: Emergency Medical Services
GPS: Global Positioning System
RFID: radio frequency identification
START: Simple Triage And Rapid Treatment
WIISARD: Wireless Internet Information System for medicAl Response in Disasters
PHI: protected health information
HIPAA: Health Insurance Portability and Accountability Act
UI: user interfaces

Received: July 8, 2012
Accepted: September 27, 2012

Online publication: July 26, 2013

doi:10.1017/S1049023X13008686

Abstract

Introduction: Electronic medical records (EMRs) are considered superior in documentation of care for medical practice. Current disaster medical response involves paper tracking systems and radio communication for mass-casualty incidents (MCIs). These systems are prone to errors, may be compromised by local conditions, and are labor intensive. Communication infrastructure may be impacted, overwhelmed by call volume, or destroyed by the disaster, making self-contained and secure EMR response a critical capability.

Report: As the prehospital disaster EMR allows for more robust content including protected health information (PHI), security measures must be instituted to safeguard these data. The Wireless Internet Information System for medicAl Response in Disasters (WIISARD) Research Group developed a handheld, linked, wireless EMR system utilizing current technology platforms. Smart phones connected to radio frequency identification (RFID) readers may be utilized to efficiently track casualties resulting from the incident. Medical information may be transmitted on an encrypted network to fellow prehospital team members, medical dispatch, and receiving medical centers. This system has been field tested in a number of exercises with excellent results, and future iterations will incorporate robust security measures.

Conclusion: A secure prehospital triage EMR improves documentation quality during disaster drills.

DeMers G, Kahn C, Johansson P, Buono C, Chipara O, Griswold W, Chan T. Secure scalable disaster electronic medical record and tracking system. ***Prehosp Disaster Med.*** **2013;28(5):498-501.**

Introduction

This is a technical report describing a newly developed electronic system for use in tracking and coordinating patient management in a mass-casualty incident (MCI) or disaster setting. Current convention is to utilize color-coded paper triage tags, which are attached physically to a victim's clothing or extremity in a linear process. There are a number of triage methods and systems that apply to different populations and situations.[1-4] Medical response to disaster scenes may involve MCIs requiring a rapid, accurate patient assessment and triage capability. Acute management and disposition of these injured persons is often fraught with challenges. In the setting of overwhelming numbers of victims, medical personnel must contend with time constraints, austere settings, and frequently with limited personnel support or resources.

Paper-based triage systems are costly to maintain updated versions, vary widely in manufacture design, are prone to input errors, and data may be lost during transport of the victim. In addition, space is limited on traditional tags for re-triaging patients should their conditions change while awaiting transport. Paper tags may also be compromised by local adverse conditions such as exposure to water making the tags illegible. Information provided on the tags is not secure and may be unintentionally disclosed to third parties. These and other inadequacies often result in failure to take advantage of the documentation capabilities of the tag.

The current method of tag triage is a static and fragmented information repository. Real-time and dynamic information regarding victim status is critical to the management of field medical care. Medical command oversight must coordinate timely intelligence on the number and acuity of casualties to match availability of assets, such as on-scene providers, ambulance locations, and area hospital capacities.[5,6] Real-time information is

also critical to determining the appropriate patient disposition, depending on the injury pattern and available resources at destination.

Current Emergency Medical Services (EMS) communication to hospitals relies on nonsecure radio channels. Many prehospital personnel rely on 800 MHz trunked public safety radio systems to communicate with medical control. Victims of MCI are triaged with paper tags and radioed in to hospital receiving centers via base station coordinators who in turn activate disaster protocols within their respective institutions. Communication infrastructure may be impacted, overwhelmed by call volume, or destroyed by the disaster, making self-contained and secure incident prehospital electronic medical record (EMR) response a critical capability.

The Wireless Internet Information System for medicAl Response in Disasters (WIISARD) research group was formed in 2003 via a grant from the National Library of Medicine to address deficiencies in patient tracking and care coordination at mass-casualty incidents. In coordination with local EMS authorities, and in evolution through multiple full-scale drill deployments, the group has developed a patient tracking system integrated with an EMR that collects medical information in electronic form. Persisting information electronically reduces the likelihood of accidental loss and makes it feasible to share this information with rescuers, incident commanders, and casualty receiving centers. Smart phone EMR software emulates the standard paper triage tag and provides an option to include additional free text information. Information may be added to the EMR in a tiered approach as time and indications dictate. Access to prehospital information is valuable throughout the care of the patient after transport to a medical receiving facility. For example, if patients are no longer able to provide medication lists, allergies, and medical conditions upon arrival at a hospital, subsequent care could be suboptimal.

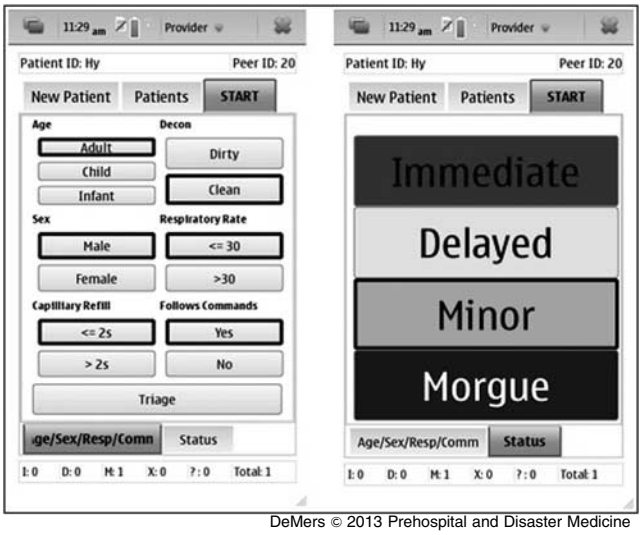
This report outlines the design, development, and operation of a secure patient tracking and coordination system, and highlights technical components of the system. Further technical details are available from the authors.

Report

WIISARD System Components

The WIISARD system uses off-the-shelf, 3G (third generation) capable smart phones with 802.11 wireless transmission capabilities for communication and radio frequency identification (RFID) readers for patient tracking, with an open source operating system. Data can be uploaded to a central WIISARD server. A peer-to-peer data dissemination scheme enables WIISARD to disseminate medical information reliably without requiring pre-existing infrastructure, even in dynamic wireless environments such as the ones observed during MCIs. WIISARD adopts the following technologies to support patient tracking and information dissemination.

Tagging—WIISARD enables the tracking of victims from the initial incident until they are transported to hospitals to further care. In WIISARD, passive RFID tags are used to identify patients. WIISARD takes advantage of global positioning systems (GPS) capabilities in modern phones to track both providers and victims. As providers carry the phones, their location can be directly determined using the phone's GPS. The location of a victim is updated every time when a provider scans their RFID tag. This offers a lightweight approach to track victims during MCI.



DeMers © 2013 Prehospital and Disaster Medicine

Figure 1. Provider WIISARD UI Component
Abbreviations: UI, user interface; WIISARD, Wireless Internet Information System for medicAl Response in Disasters

Role-tailored User Interfaces and EMR—WIISARD provides role-tailored user interfaces (UI) to facilitate efficient information collection and visualization. WIISARD implements an electronic version of the START protocol. Although there are limited data to support the use of any particular triage system over another, WIISARD utilizes START due to the system's ubiquity and previous validation testing. After a patient is tagged, first responders can triage the patient using the Provider UI component. The Provider UI is tailored to support incremental collection of information and patient re-triage, capabilities that are difficult to support using standard paper tags (Figure 1).

Additional UIs have been developed to support the transport and command and control roles. The transport UI allows the transport officer to send patients to receiving hospitals subject to the availability of ambulances. In turn, the command center provides the incident commander an overview of the situation: all patient information, summary statistics about the progress of response, and GPS coordinates for both providers and victims.

Communication Capabilities—Reliable communication during disaster response faces two key challenges. First, the system must operate in a dynamic environment, where providers and patients are mobile and radio characteristics may change as equipment arrives on scene. Second, during disasters there will be limited networking infrastructure. As a result, network disconnections and partitions will be frequent.

To address these challenges, a peer-to-peer architecture was adopted in which a peer acts as both client and server using a gossip-based solution. A gossip protocol works by having each node "gossip" the information it hears from its neighbors until all nodes in the network have this information. Gossip protocols have the inherent advantage of being local protocols in which

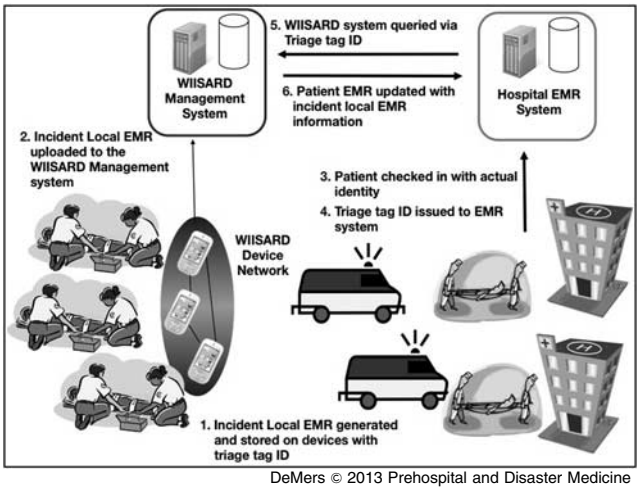
https://doi.org/10.1017/S1049023X13008686 Published online by Cambridge University Press

WIISARD Future Security Opportunities
Radio link encryption (e.g., WPA2-PSK)
Application data encryption
Provider authentication
Limited patient identity entry
Blacklisting of compromised devices
Centralized device management for: • Updated user credentials and encryption keys • EMR data uploading and flushing

DeMers © 2013 Prehospital and Disaster Medicine

Table 1. Summary of Future Security Components for WIISARD

Abbreviations: EMR, electronic medical record; WIISARD, Wireless Internet Information System for medicAl Response in Disasters



DeMers © 2013 Prehospital and Disaster Medicine

Figure 2. Flow of Incident Local EMR Information from the WIISARD System to the Hospital's EMR System

Abbreviations: EMR, electronic medical record; WIISARD, Wireless Internet Information System for medicAl Response in Disasters

each node communicates only with the nodes within its communication range, without requiring connectivity to a central server. For a complete description of the protocol and evaluation the readers may refer to Chipara et al.[7]

Victim Patient Data Concerns

An obvious benefit of disaster triage/EMR systems is access to accurate records of prehospital interventions to assist throughout the patient's continuum of care in the hospital. Current prehospital systems are not standardized and range from paper documentation to fully integrated EMRs that become part of the patient's hospital record. Information regarding medical history such as allergies, resuscitation preference (code status) and medications often is not immediately available for emergency department management of acute patients. As prehospital triage/EMR systems evolve to incorporate these data and protected health information (PHI) in the prehospital EMR, concerns arise for security.

Medical Management of PHI

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 provides a series of administrative, physical, and technical requirements for PHI to assure its confidentiality, integrity, and availability. Transfer of PHI for patient care related issues is allowed under the act, but safeguards are required to prevent unintentional disclosure of information to parties not involved in the direct care of patients. HIPAA was not designed to address disaster situations though the intent to protect sensitive data is a major concern in the WIISARD design and development. Information security standards, recommendations and guidelines from the National Institute of Standards and Technology (NIST) should be followed whenever possible in the design of a secure disaster EMR system.[8] Further security components will be added to WIISARD in the future (Table 1).

Integration With Hospital EMR Systems

The incident EMR information collected by the WIISARD system during triage and prehospital treatment is uploaded to the secure WIISARD management system via, for instance, a secure cellular connection. This occurs periodically during the incident response if cellular coverage is sufficient at the scene, or whenever the devices get within coverage range during transport to the hospital. Since typically all the WIISARD devices engaged during the incident will carry the same, synchronized, EMR data it is enough if only a subset of the devices uploads the incident EMRs to the central WIISARD management system.

Once patients arrive to a hospital, the hospital providers will identify the patients via their triage tag RFID during check-in procedures. At this point the incident EMR can be retrieved from the WIISARD management system and associated, or merged, with the patients' actual EMR used by the hospital. The inclusion of the incident EMR will be done according to HIPAA-compliant methods deployed by the hospital. This way, patients' PHI records are never released or even visible to the WIISARD system, but only updated with the prehospital care information within the incident EMR. Neither is the actual patient's full identity associated with the incident EMR, which relaxes the level of security needed for the WIISARD system. Figure 2 illustrates the flow of EMR data described above.

Conclusion

Medical information gathered at disaster scenes may be obtained in a tiered fashion by prehospital personnel. These data are valuable throughout the care of the patient, from first response in the field through transport to a medical receiving facility and inpatient care. The prehospital EMR for disaster response is becoming more robust with further potential use by medical providers at receiving facilities. Security and procedural measures are needed to prevent disclosure of PHI in disaster prehospital incident EMRs.

Acknowledgment

The authors wish to thank the City of San Diego, California Fire Department for participation in drill exercises.

References

1. Garner A, Lee A, Harrison K, Schultz CH. Comparative analysis of multiple-casualty incident triage algorithms. *Ann Emerg Med*. 2001;38:541-548.
2. Kahn CA, Schultz CH, Miller KT, et al. Does START triage work? An outcomes assessment after a disaster. *Ann Emerg Med*. 2009;54(3):424-430, 430 e421.
3. Kahn CA, Lerner EB, Cone DC. Triage. In: Koenig KL, Schultz CH, eds. *Koenig and Schultz's Disaster Medicine: Comprehensive Principles and Practices*. Cambridge, UK: Cambridge University Press; 2010:174-183.
4. Garner A. Documentation and tagging of casualties in multiple casualty incidents. *Emerg Med (Fremantle)*. 2003;15(5-6):475-479.
5. Bouman JH, Schouwerwou RJ, Van der Eijk KJ, van Leusden AJ, Savelkoul TJ. Computerization of patient tracking and tracing during mass casualty incidents. *Eur J Emerg Med*. 2000;7(3):211-216.
6. Teich JM, Wagner MM, Mackenzie CF, Schafer KO. The informatics response in disaster, terrorism, and war. *J Am Med Inform Assoc*. 2002;9(2):97-104.
7. Chipara O, Plymoth AN, Liu F, Huang R, Evans B, Johansson P, Rao R, Griswold WG. "Achieving Reliable Communication in Dynamic Emergency Responses" American Medical Informatics Association Annual Symposium (AMIA 2011).
8. Padgette L, Scarfone K, Chen L. Guide to Bluetooth Security Recommendations of the National Institute of Standards and Technology. Special Publication 800-121 Revision 1. National. Institute of Standards and Technology. Gaithersburg, Maryland, USA; 2012: 1-47.