Weathering the Storm: Electronic Health Records and Disaster Recovery

Laura M. Cascella, MA

Natural disasters, although devastating, offer opportunities to examine various aspects of disaster planning, preparedness, and response — including those related to healthcare. Specifically, several major disasters over the past decade have provided a glimpse of the many ways in which electronic health records (EHRs) are capable of transforming disaster recovery efforts for the healthcare community.

In 2005, thousands of paper health records were destroyed when Hurricane Katrina ravaged the Gulf Coast. However, the Department of Veterans Affairs (VA), which had implemented an EHR system, was able to safeguard its health records and transfer patients and their pertinent information to other VA medical centers when the disaster struck.1

In 2011, a newly implemented EHR system allowed St. John’s Regional Medical Center and its affiliated practices to quickly recover and access patient records after a tornado severely damaged Joplin, Missouri.2

In 2012, EHRs and health information exchange (HIE) facilitated uninterrupted care and prevented widespread loss of patient health information as Hurricane Sandy pummeled the Mid-Atlantic and Northeast.3

These examples highlight the utility of EHRs in disaster recovery. Unlike paper records, which can be easily destroyed and incredibly difficult to rebuild, EHRs can:

- Protect patient data and other important information, even if physical structures are damaged or lost
- Allow healthcare providers and organizations to quickly transfer health records for patients who are evacuated to other facilities
- Prevent the need to rely on patient recollection and memory to gather critical health information
- Facilitate the continuity of care during and after a disaster

EHR Considerations for Disaster Recovery Planning

For healthcare organizations and practices to realize the full potential of EHRs in disaster situations, they need to consider various aspects of their systems and include processes related to information technology (IT) management as part of their emergency preparedness plans.4,5,6,7
Some of these considerations include:

- **Onsite Safety**
  - Is your IT equipment (e.g., servers, laptops, etc.) kept in the safest place possible within your practice? For example, if you have a multi-level office, is your IT equipment stored on a higher floor to prevent damage from flooding?
  - Do you have a protocol for shutting down all systems prior to an impending disaster?
  - Who in the practice is responsible for overseeing IT equipment and procedures?

- **Accessibility**
  - Does your practice have a backup generator to restore power during an emergency or outage?
  - If so, does the backup power source have the capability to restore power to your IT infrastructure?
  - Does your practice have a detailed protocol for how to handle loss of Internet connectivity?

- **Data Backup**
  - How is information from your practice’s EHR system backed up? Is the information stored onsite or at an offsite data warehouse?
    - If onsite, how will you recover data if a disaster — such as a fire — destroys the office structure/IT equipment?
    - If offsite, what is the appropriate procedure for accessing the backup data?
  - How often are data backed up?

- **Interoperability**
  - If your practice is part of a larger organization, is your system compatible with other local and regional systems?
  - Can the system facilitate smooth transfer of patient records if necessary?
  - Is your practice participating in an HIE?

- **Emergency Procedures**
  - Does your practice have a written procedure for staff to use in the event of system failure or inaccessibility?
  - Are hard copies of the emergency procedure available in the event that the practice’s electronic systems are not accessible?
o How will staff continue to provide care if the EHR system is not available?
  o How will staff update the system once it is back online?

• Training
  o Are providers and other staff members in the practice trained for emergency situations, including natural disasters and other types of emergencies?
  o Does training occur when new technology is introduced and when procedures and workflow processes are updated?
  o Do providers and staff members know their roles and responsibilities and appropriate actions to take during an emergency?

• Vendor Support
  o Is your EHR/data warehouse vendor focused on customer service?
  o What services does your vendor supply in the event of a disaster?
  o Are these services clearly defined in a service agreement?

These questions provide some general thoughts to consider when including an EHR system as part of your practice’s emergency preparedness protocols. For more information about incorporating an EHR system into your disaster recovery planning, visit [http://www.healthit.gov/providers-professionals/faqs/how-do-i-develop-recovery-plan-event-system-failures-or-loss-internet-a](http://www.healthit.gov/providers-professionals/faqs/how-do-i-develop-recovery-plan-event-system-failures-or-loss-internet-a).

**Conclusion**

When used appropriately, EHR systems have proven beneficial in disaster recovery. Over the past decade, these systems have weathered major crises and shown their resilience in the face of disaster. When incorporated into a comprehensive disaster recovery plan, EHRs “will help sustain practices and enable the ability to provide essential health care services post-disaster when patients may be most vulnerable.”8
Endnotes


