MedPro Group
a Berkshire Hathaway company

Weathering the Storm: Electronic Health Records and Disaster Recovery

Laura M. Cascella, MA, CPHRM

PEACE OF MIND | EXPERTISE | CHOICE | THE MEDPRO GROUP DIFFERENCE

Natural disasters, although often devastating, offer opportunities to examine various aspects of emergency preparedness, including those related to healthcare. The large-scale adoption of electronic health records (EHRs) over the past 2 decades has revealed how this technology is capable of transforming disaster recovery efforts for healthcare facilities. For example, EHR systems were instrumental in helping safeguard and transfer patient health data during Hurricanes Katrina, Sandy, Harvey, and Irma.[1]

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

The majority of healthcare organizations and practices have implemented EHR systems; thus, healthcare administrators, providers, support staff, and technical staff should consider how to carefully and thoughtfully incorporate this technology into disaster response plans.

Electronic Health Record Considerations for Disaster Planning

Establishing a comprehensive disaster recovery plan that includes guidance and strategies related to EHR systems (as well as other health information technologies) is crucial for healthcare organizations of all types and sizes.

The HIPAA Security Rule requires a data backup plan, a disaster recovery plan, and an emergency mode operation plan . . .”

The HIPAA Security Rule requires covered entities (CEs) to develop contingency plans for responding to emergencies/disasters and safeguarding electronic protected health information (ePHI). Further, CEs “need to have policies and procedures in place that cover emergency response where systems containing PHI are damaged. This could include a fire, system failure, or natural disaster.”[2]

As part of contingency planning, HIPAA requires a data backup plan, a disaster recovery plan, and an emergency mode operation plan; the Security Rule also advises CEs to develop testing and revision procedures and to conduct an analysis of applications and data criticality.[3]

When determining how to address EHR systems as part of emergency preparedness and response planning — and as part of overall health information technology (IT) management — various factors should be considered.[4] Examples of these considerations include:

- **Onsite safety**
  - Is onsite IT equipment (e.g., servers, laptops, networking devices, etc.) kept in the safest place possible within your facility? For example, if you have a multi-level office, is your IT equipment stored on a higher floor to prevent damage from flooding? Identifying and assessing the types of hazards that could affect your organization will help determine appropriate onsite safety measures.
  - Does your organization have a protocol for shutting down all systems prior to an impending disaster?
  - Have appropriate individuals in your organization been delegated the responsibility of overseeing IT equipment and procedures?

- **Accessibility**
  - Does your facility have a backup generator to restore power during an emergency or outage?
  - Is adequate fuel maintained for the generator, and is the generator tested monthly?
  - Does your facility's backup power source have the capability to restore power to your IT infrastructure?
  - Does your facility have a detailed protocol for how to handle loss of internet connectivity?
- **Data backup**
  - How is information from your organization's EHR system backed up? Is the information stored onsite/locally or offsite (e.g., at a remote data warehouse or with a cloud-based service)?
    - If onsite/locally, how will you recover data if a disaster — such as a hurricane or flooding — damages or destroys the data backups?
    - If offsite, what is the appropriate procedure for accessing the data backups? Who is authorized to do so?
  - Are data routinely and automatically backed up (e.g., every 24 hours or more frequently)?
  - Do data backups overwrite previous backups? If so, does your IT vendor have protocols for accessing previous versions of records?
  - Does your organization regularly review data backups to verify their integrity?

Risk Tip

Implementing best practices for backing up data is crucial for natural disasters and other types of crises, such as cyberattacks. In the event that data are stolen, ransomed, or corrupted — or that systems are shut down — having reliable backup data can make a monumental difference in recovery and continuity of care.

  - What is the process for recovering data and applications?
  - Does your organization have a "read-only" backup EHR system that is updated frequently? Have providers and staff members been trained on when and how to active the read-only system?

- **Interoperability**
  - If your facility is part of a larger healthcare organization, is your EHR system compatible with other local and regional systems?
  - Can your EHR system facilitate smooth transfer of patient records if necessary?
  - Are protocols in place for transferring ePHI without violating HIPAA regulations?
  - Is your practice participating in a health information exchange?
- **Emergency procedures**
  - Does your organization have a written procedure for staff to use in the event of system failures or inaccessibility?
  - Are paper copies of the emergency procedure available in case the organization's electronic systems are not accessible?
  - Are policies in place to ensure accurate patient identification during system downtimes?
  - Is a contingency plan in place for documenting patient care and other important information if the EHR system is unavailable? Are safeguards in place to ensure HIPAA compliance for paper documentation?
  - Have procedures been established for updating the EHR system with data from paper documentation?
- **Training**
  - Are healthcare providers and other staff members in the organization trained for emergency situations, including natural disasters and other types of emergencies?

  - Does training occur when new technology is introduced and when procedures and workflow processes are updated?
  - Do healthcare providers and staff members know their roles/responsibilities and appropriate actions to take during an emergency?
  - Have providers and staff members received training on paper documentation protocols in the event that EHR systems or other technologies are unavailable?

- **Vendor support**
  - Is your EHR/data warehouse vendor focused on customer service?
  - What type of services/support does your vendor supply in the event of a disaster?
  - Are emergency preparedness and disaster recovery services clearly defined in a service agreement?
  - What data security measures has your vendor implemented?
  - How often does your vendor test its data recovery processes?

These questions provide some general thoughts to consider when incorporating your EHR system into emergency preparedness protocols. For more information about including EHR systems in disaster recovery plans, visit the Office of the National Coordinator for Health Information Technology at HealthIT.gov and see the *Contingency Planning* SAFER Guide.

Take-Away Message

EHR systems can facilitate disaster recovery, and they can "help sustain practices and enable the ability to provide essential health care services post-disaster when patients may be most vulnerable."[5] Over the years, EHR systems have weathered major crises and shown their resilience in the face of disaster.

To realize the full potential of EHRs as a vital component of emergency planning, healthcare organizations should consider environmental and technical factors associated with these systems and optimize safeguards related to data preservation, recovery, and exchange.

Endnotes

[1] Abir, M., Mostashari, F., Atwal, P., & Lurie, N. (2012, Dec.). Electronic health records critical in the aftermath of disasters. *Prehospital and Disaster Medicine*, 1–3; MedCity News. (2012, Oct. 30). Hurricane Sandy proves the value of health IT infrastructure, state info exchanges. Retrieved from http://medcitynews.com/2012/10/hurricane-sandy-underscores-new-yorks-health-information-exchange-and-data-storage-logistics/; Gettinger, A. (2017, November 15). Reflections from a health IT perspective on disaster response. *Health IT Buzz*. Office of the National Coordinator for Health Information Technology. Retrieved from www.healthit.gov/buzz-blog/health-it/reflections-health-perspective-disaster-response/; Lichtenwald, I. (2017, September 22). How recent hurricanes expose remaining gaps in healthcare IT. *Health Data Management*. Retrieved from www.healthdatamanagement.com/opinion/how-recent-hurricanes-expose-remaining-gaps-in-healthcare-it

[2] Snell, E. (2018, January 24). Why providers need a disaster recovery plan for EHR security. HealthIT Security. Retrieved from https://healthitsecurity.com/news/why-providers-need-a-disaster-recovery-plan-for-ehr-security

[3] HIPAA Privacy and Security Rule, 45 C.F.R. § 164.308(a)(7)(i).

[4] Abir, et al. Electronic health records critical; Harris, B. (2012, Oct. 29). 3 health IT must-haves for natural disaster preparedness. *Healthcare IT News*. Retrieved from www.healthcareitnews.com/news/3-health-it-must-haves-natural-disaster-preparedness; Coughlin, B. (2012, Nov. 21). In the wake of Hurricane Sandy: Health IT 1, paper records 0. *Health IT Buzz*. Office of the National Coordinator for Health Information Technology. Retrieved from www.healthit.gov/buzz-blog/ehr-case-studies/hurricane-sandy-health-information-technology/; The Office of the National Coordinator for Health Information Technology. (2016, July). *SAFER self-assessment: Contingency planning*. Retrieved from www.healthit.gov/sites/default/files/safer/guides/safer_contingency_planning.pdf; Tennant, R. M. (2019, August 1). *Backing up your patient data: A compliance and business imperative*. Medical Group Management Association. Retrieved from www.mgma.com/data/data-stories/backing-up-your-patient-data-a-compliance-and-bus; Smith, D. (2019, January 10). *How often should medical/dental offices backup data & why data backup is important*. Integrity Systems & Solutions. Retrieved from www.integrityss.com/blog/how-often-should-medical-dental-offices-backup-their-data-and-why-its-important

[5] Abir, et al. Electronic health records critical.