Compliance Today - July 2025

Jerry Kaner (jkaner@ciphertex.com) is the Founder and CEO of Ciphertex Data Security in Chatsworth, CA.

Maintaining compliance in the face of disaster

by Jerry Kaner

While some threats can be prevented, natural disasters are not among them. These crises put patients—and their data—at risk. Beyond structural damage and dangerous conditions, they expose IT vulnerabilities and create lucrative opportunities for threat actors to kick a facility when it's down. Unfortunately, natural disasters are not a valid excuse for HIPAA violations. Noncompliance still risks costly fines, operational disruptions, and reputational turmoil.

According to the World Meteorological Organization, the number of these events has increased fivefold in the last 50 years.[1] That said, it is only a matter of time before disaster strikes your organization. Are you prepared enough to remain compliant and protect your patients' privacy when it does?

The shift to EMRs: Progress and persistent vulnerabilities

The rapid digital transformation of the healthcare industry has fundamentally changed how organizations prepare for and are affected by natural disasters. In the past, a lack of centralized, portable, and easily recoverable patient data significantly hindered both immediate disaster response and long-term recovery. In 2005, for example, many healthcare facilities had yet to implement electronic medical records (EMRs), relying entirely on paper-based systems. When Hurricane Katrina struck, this dependence on physical records led to catastrophic losses.

Floodwaters and structural damage rendered thousands of patients' charts unreadable at best, wiping out vital details about treatment histories, medication regimens, and allergies. This strained hospitals receiving displaced patients, as they were forced to conduct redundant tests or make clinical decisions with limited access to important information. In contrast, early EMR adopters were able to weather the storm more easily. The Veterans Administration already had a robust system in place when Katrina hit, and its providers were able to access the records of displaced patients from outside the disaster zone.[2]

The value of EMRs was demonstrated again in 2011 when an EF5 tornado devastated the community of Joplin, MO., and left St. John's Regional Medical Center severely damaged. A mere three weeks prior, the facility had completed its transition to electronic recordkeeping. Although some paper records and X-rays were lost, the switch meant that most patient information remained intact and accessible. Less than a week after the tornado, the hospital's staff was operating again in a temporary medical unit with full access to digital records.[3]

Broad adoption of EMR systems and cloud technology has helped mitigate some of the challenges posed by natural disasters, allowing healthcare providers to access patient information from off-site locations even when local systems are compromised. However, the effectiveness of these tools depends on factors like connectivity, power, and the stability of third-party providers. When supporting infrastructure fails, digital records are far less useful.

Infrastructure failures reveal gaps

During Hurricane Sandy in 2012, hospitals in New York and New Jersey faced severe flooding that knocked out power and local servers, leaving some facilities unable to access EMRs.[4] In 2017, Hurricane Maria further demonstrated the fragility of healthcare IT systems in prolonged disaster scenarios. The storm left much of Puerto Rico without power for months, rendering digital records inaccessible at many healthcare facilities.[5] More recently, the Los Angeles wildfires caused widespread power outages and infrastructure damage, leading clinics to close and prompting the evacuation of patients at long-term care facilities.[6] Clearly, while EMRs have improved healthcare resilience, they are *not* a fail-safe solution in disaster scenarios. Cloud storage alone is insufficient if network connectivity is disrupted, and even the most advanced digital infrastructure can be debilitated by power failures, damaged servers, or cyberthreats. Furthermore, without seamless data exchange, providers may still face delays or discrepancies in patient records, complicating disaster response and potentially putting patients at risk.

Steps for maintaining security and compliance during a disaster

Planning ahead (again and again)

Although healthcare systems cannot prevent natural disasters, they can prepare for them. Not doing so puts organizations at risk of noncompliance. Under HIPAA, covered entities must maintain retrievable copies of electronic protected health information (ePHI) and have a tested disaster recovery protocol in place.

The first step is to ensure you have a comprehensive plan outlining specific procedures for protecting data in an emergency, including considerations for alternative work arrangements in case a facility is rendered inaccessible. Ensure that the necessary steps for securing sensitive information and maintaining compliance both on-site and remotely are clear and easily accessible to those who may need to execute them.

Team members must understand their roles, as even the most well-designed plan will be ineffective if staff members are unclear on what actions to take. Conducting training sessions, tabletop simulations, and live drills can help clarify individual responsibilities and reveal organizational weaknesses. Likewise, proactively testing backup and recovery processes under controlled conditions ensures that key system functionalities are working properly before they are needed.

Beyond general preparedness exercises, regular compliance audits and after-action reviews should be conducted to evaluate how well teams follow protocols during simulations. These audits should also assess data integrity, ensuring patient records remain complete, accurate, and retrievable across all backup systems. Even minor data corruption or system failures can compromise compliance, leading to missing or altered records that hinder patient care and trigger regulatory scrutiny.

Coordinating with third-party vendors is also critical, and not just because of the impact a local natural disaster can have on a healthcare organization. Vendors themselves are not immune to these events and if one providing cloud storage, data processing, or other essential services is impacted, access to patient information could still be compromised. Compliance officers should review business associate agreements to confirm that vendors have adequate security and redundancy measures in place.

It is vital to understand that preparation—and all it involves—is not a one-and-done activity. Too often, organizations rely on outdated strategies that fail to address evolving risks. Annual risk assessments, ongoing staff education, and regular audits of third-party vendors must be part of a hospital’s long-term compliance strategy. A reactive approach to disaster preparedness leaves patient data vulnerable. A proactive, continuously refined strategy ensures facilities maintain compliance, protect patient privacy, and sustain operations even in challenging circumstances.

Diversifying data storage

As demonstrated by the examples mentioned earlier, no single storage solution can guarantee uninterrupted access to patient data during a disaster. The need for data redundancy and secure backup systems cannot be overstated. Cloud solutions have been widely adopted by the industry due to their cost-savings, scalability, and geographic redundancy. Unfortunately, power, internet, and service provider outages can interfere with access.

Only storing data on-site creates its own risks, as servers cannot easily be moved but can be destroyed by a fire or flood. Although hard drives could be removed and taken elsewhere without robust encryption mechanisms, there is a risk that they could fall into the wrong hands and expose vast amounts of patient data.

In any case, when providers lose access to ePHI, they face regulatory scrutiny, fines, and legal action. For example, a healthcare provider that cannot retrieve patient records due to power outages or network disruptions may be found to be noncompliant. A hybrid approach that leverages both on-premises and cloud storage reduces compliance risks by ensuring multiple access points to patient data—even when primary systems fail.

Incorporating portable solutions, such as secure network-attached storage, into backup strategies can bolster resilience. They allow hospitals and clinics to maintain critical data backups that can be accessed quickly in the event of network failures. The devices also offer the ability to quickly move data to a safer location without compromising integrity; this feature is especially valuable for those operating in disaster-prone regions where evacuations are a factor.

Leveraging encryption

Regardless of whether data is stored on-site, in the cloud, or on a portable server, encryption (both at rest and in transit) is imperative for safeguarding patient records. Without it, backup files, removable drives, and even transmitted data could be intercepted or compromised, increasing the risk of HIPAA violations.

Not all encryption is created equal. Hardware encryption is built directly into physical storage devices, such as encrypted external drives or self-encrypting solid state drives, offering faster performance and better resistance to brute-force attacks. These operate independently of the host system, reducing exposure to malware and keylogging attacks. Additionally, some storage solutions offer an extra level of physical security with custom-designed hardware encryption keys.

On the other hand, software encryption relies on applications to encrypt data, providing more flexibility but potentially being more vulnerable to cyberthreats if the encryption keys are not properly secured. A strong data protection strategy should leverage both.

Recognizing that an organization’s crisis is a cybercriminal’s dream

Although natural disasters pose immediate risks to patient safety and operations, for threat actors, they present a lucrative opportunity. IT security often becomes a secondary concern when an organization scrambles to restore services and maintain continuity of care. Cybercriminals recognize this and launch attacks, knowing that overstretched teams are likelier to overlook security warnings or make mistakes under pressure.

One of the most significant threats post-disaster is ransomware. With systems down and urgent medical needs at stake, some organizations have been forced to pay a hefty price just to regain control of their records; however, data may still be leaked. Phishing is a leading vector for these attacks, with criminals posing as IT team members or executive leadership to trick employees into providing their login credentials. In such high-stress environments, even seasoned professionals can fall victim to increasingly sophisticated scams.

Another major concern comes in the form of malicious insiders. During disasters, organizations frequently bring in temporary personnel or relocate patients, creating a need for flexible yet secure data access. Without strict controls in place, this can lead to breaches as unauthorized individuals gain entry to sensitive systems.

Building cyber resilience

Continuously monitoring cybersecurity risks and revisiting protocols helps reveal vulnerabilities such as outdated software or inadequate access controls before they become a target for threat actors. Organizations also benefit from proactively educating their staff on emerging threats, common attack vectors, digital hygiene, and the need to report suspicious activity.

Network segmentation helps prevent the spread of ransomware and malware by isolating backup systems and sensitive databases from the broader hospital network. Another critical safeguard is multi-factor authentication (MFA). Countless data breaches have proven that passwords alone are insufficient. Implementing MFA lowers the odds of unauthorized access even if credentials are compromised.

Additionally, establishing read-only emergency access to electronic health records for essential staff can prevent workflow bottlenecks without compromising compliance. In parallel, manual documentation protocols should be outlined in case systems go offline, allowing for continued patient care without unnecessary compliance risks.

Can your organization weather the storm?

The question isn't *if* another disaster will strike; it is *when*. The real concern is whether the healthcare sector has the infrastructure, policies, and risk management strategies to minimize the impact when it does.

Past incidents have made one thing clear: Organizations that invest in strong infrastructure, diversified storage, and cybersecurity recover faster with less data loss. Those that don't face prolonged downtime, compliance violations, reputational damage, and, in some cases, permanent loss of critical patient records. Waiting until something goes wrong isn't an option; protecting ePHI isn't just a compliance issue; it is a matter of patient safety, regulatory responsibility, and the long-term stability of healthcare institutions.

Takeaways

- Natural disasters expose healthcare IT vulnerabilities, threatening both patient safety and data security; however, HIPAA compliance is still mandatory even during crises.
- While digital records help mitigate disruption, their effectiveness depends on stable power, connectivity, and infrastructure.
- Disaster preparedness must be continuous; regular simulations, audits, and updated protocols are essential for maintaining compliance and readiness.
- Relying solely on cloud or on-premises systems is risky; a hybrid model ensures better accessibility during outages.
- Cyberattacks spike during disasters as threat actors exploit weakened defenses; having strong access controls, employee awareness, multi-factor authentication, and segmented networks helps reduce the risk of breaches.

[1] World Meteorological Organization, "Weather-related disasters increase over past 50 years, causing more damage,

fewer deaths," news release, August 31, 2021, https://wmo.int/media/news/weather-related-disasters-increase-over-past-50-years-causing-more-damage-fewer-deaths.

[2] Steven H. Brown et al., "Use of Electronic Health Records in Disaster Response: The Experience of Department of Veterans Affairs After Hurricane Katrina," *American Journal of Public Health* 97, Supplement_1 (April 2007): S136–S141, https://doi.org/10.2105/AJPH.2006.104943.

[3] Nicole Lurie and Farzad Mostashari, "Electronic Health Records Prove to be Invaluable After Crisis," Health IT Buzz, June 22, 2011, https://www.healthit.gov/buzz-blog/ehr-case-studies/electronic-health-records-prove-invaluable-crisis.

[4] Sheilla L. Rodríguez-Madera et al., "The impact of Hurricane Maria on Puerto Rico's health system: post-disaster perceptions and experiences of health care providers and administrators," *Global Health Research and Policy* 6, (November 2021): 44, https://doi.org/10.1186/s41256-021-00228-w.

[5] Stephanie Baum, "Hurricane Sandy proves the value of health IT infrastructure, state info exchanges," *MedCity News*, October 30, 2012,https://medcitynews.com/2012/10/hurricane-sandy-underscores-new-yorks-health-information-exchange-and-data-storage-logisticshttps://medcitynews.com/2012/10/hurricane-sandy-underscores-new-yorks-health-information-exchange-and-data-storage-logistics.

[6] Emily Alpert Reyes, Bernard J. Wolfson, and Molly Castle Work, "Doctors, nurses press ahead as wildfires strain L.A.'s healthcare," *Los Angeles Times*, January 10, 2025, https://www.latimes.com/california/story/2025-01-10/la-wildfires-strain-la-healthcare.