Codify
BY AAPC

Health Information Compliance Alert

Disaster Planning: Protect Yourself and Your EHR Before Disaster Strikes

Tip: Get your physical security in check after the hurricane.

Hurricane season is upon us, and each new storm brings its own set of woes. The critical importance of steady and safe healthcare is essential to combat such chaos, but what happens when the electricity is out, the infrastructure is broken, and the systems are down? Plan now to avoid frustration later.

Do These Things Before the Chaos

The protection of protected health information (PHI) and electronic protected health information (ePHI) falls under HIPAA, ensuring that patients' privacy and security aren't compromised. But it's more than that because "the availability and integrity of such data is what allows healthcare providers to make educated decisions on patients' behalf," cautions **Brand Barney, HCISPP, CISSP, QSA**, security analyst with Security Metrics inOrem, Utah.

"In all honesty, most providers I know get overly anxious when the power is down for even a few minutes and they don't have access to their charts. So, when you are juggling HIPAA requirements, hackers, and security issues during and after an emergency, thearising situations can seem insurmountable," explains Barney.

Smart and detailed preparation from encryption to staff training to offsite storage ensures less of a headache in the aftermath. Take a look at these seven tips from Barney on what to do before catastrophe:

1. Encrypt, encrypt, encrypt. "If you do have a breach in your networks, or if a device containing PHI is stolen, proper encryption can be a lifesaver," Barney points out. "If your data is properly encrypted using industry-accepted encryption strengths, you don't have a breach. And it's also a requirement for HIPAA."

2. Train and retain. "Your staff are your greatest asset, but can also be your biggest weakness," he maintains. "Security awareness training doesn't have to be a once-a-year event, or happen only when there's a new hire. Make sure your staff understand that they must reasonably and appropriately restrict access to only those persons/entities with a need for access to PHI and systems."

3. Back IT up. Don't get stuck in an emergency situation. "Backing up your data and storing your backups in a safe, offsite location is essential," advises Barney. "Keep exact, retrievable copies of PHI for emergencies. This will allow for continuation of critical business processes. Remember, don't forget to encrypt those backups."

4. Revise and revisit policies often. "We often think of the [HIPAA] Privacy Rule as the only thing that has policies, but Security and Breach are equally important," he points out. "If you don't have these policies and subsequent procedures in place, it is time to get them."

5. Know your risks. Risk assessment, analysis, planning, and management are required under HIPAA, so it is mandated that you understand and study your threats and vulnerabilities. "You will be able to make educated decisions to improve your security and prevent data breaches," says Barney. "It is important to note that there is no such thing as a network in-scope environment without risk."

6. Control your physical devices appropriately. "Make sure that you have an up-to-date list of all devices that create, receive, transmit, and maintain PHI," Barney recommends. "This will help you keep track of devices and know if/when something has been replaced, tampered with, or stolen." He adds, "Your devices should be periodically inspected to ensure that tampering or device replacement has not occurred."

7. Consider cloud redundancy. "Putting your data and trust in a cloud provider can be a nerve-wracking experience," counsels Barney. "Many cloud vendors can offer you access to your data even if your physical offices have been destroyed."

Pocket This Advice for When the Dust Settles

How do you ensure your practice is safe and secure during and after a hurricane like Harvey or Irma? You implement strong compliance plans, back up your systems, follow mandates, and keep abreast of the crisis but, the most important protection might be staff education.

Vital: "Successful HIPAA security, after a disaster has occurred, comes down to training and the ability of your workforce," says **Kurt J. Long**, founder and CEO of FairWarning, Inc in Clearwater, Florida. "If employees received extensive training on security protocols and thwarting cyber attacks before the disaster occurred, then you're going to have a powerful team to secure patient data."

He continues, "For an untrained workforce, the road is going to be bumpy. If this is the case, leadership must act quickly to train their employees as best they can after the disaster has occurred. Either way, security must become an executive priority during a disaster, and employees must be held accountable."

Remember Long's checklist below for reference after a disaster:

- **Put your plan in motion.** "Execute off your business continuity plan," advises Long. "As you are rebuilding your infrastructure, elevate the priority of security."
- **Lead by example.** "If you don't have a business continuity plan, then you must rely on strong leaders to unite departments such as information security, compliance, and IT," he encourages. "United they can forge a path forward that will enable all departments to secure patient information and thwart attacks."
- **Protect your physical components.** "Ensure the physical security of your hospitals, your employees, and your data," he cautions. "During a disaster, some security protocols are left ignored, but it's important to hold employees accountable for physical security of systems."
- **Get the word out.** "Communicate with the public realistically what your plans are during the crisis," says Long. "And, what to expect afterward."

Warning: "Your 'bad days' present a massive advantage and opportunity to the bad guys," warns Barney. "Malicious entities everywhere are looking to take » advantage of, harm, and rob you and those you care for by watching for critical openings in your defenses." He adds, "During a disaster, your attention will be drawn to so many other pressing matters. I highly encourage you to consider the confidentiality, availability, and integrity of your PHI environment before, during, and after the disaster."