Hospital Computer System Crash? Prepare Now, It's Inevitable, Health Law Reporter (BNA)

BNA's Health Law Reporter™

May 31, 2018

Bloomberg BNA

Hospitals

Hospital Computer System Crash? Prepare Now, It's Inevitable

BNA Snapshot

- Hospitals can avoid system crashes and minimize harm with adequate backup systems and preparation
- Clinical staff must be prepared to treat patients “the old-fashioned way”

By Mary Anne Pazanowski

Hospital computer systems, like airplanes, shouldn't crash, but occasionally they do.

The results can be catastrophic, but there are steps health-care providers can take to avert or minimize the damage. Two attorneys who counsel hospitals told Bloomberg Law that preparation, training, and practice are the keys to surviving a systems outage that involves electronic medical records without incurring legal liability or reputational harm.

Hospitals face potentially “massive” liability, depending on the circumstances that caused the crash, Anne Murphy, a former in-house hospital counsel now in private practice at Boston's Hinckley Allen & Snyder LLP, told Bloomberg Law. C. Timothy Gary, of counsel at Nashville's Dickinson Wright and CEO of Crux Strategies, told Bloomberg Law that there is a real risk of liability exposure if a crash cuts off the clinical staff's access to patient records.

Both attorneys have helped hospitals acquire, implement, and maintain electronic health-care record systems. Crux Strategies is a global strategy firm that helps organizations and corporations navigate and avoid crises, bring about legislative changes, and resolve disputes.

Potential Exposure

Hospitals have two broad responsibilities that will be impacted by a computer system crash, Murphy said. First, they have a duty under the federal Health Insurance Portability and Accountability Act and its state analogs to ensure the security and privacy of patient health information. Second, hospitals have a duty to ensure patient safety.

A crash could affect the system's security protocols, thereby exposing patient data to dissemination outside the hospital. Under HIPAA, there is an expectation that a hospital will have an effective backup system for storing and accessing that data, so a crash could expose the hospital to liability under the laws, Murphy said.

It is more difficult to quantify a hospital's exposure for patient safety problems caused by a system crash, but the potential for professional liability exposure is significant, Murphy said.

Health-care providers are very dependent on electronic medical records that contain a patient's treatment history, including what drugs a patient currently is taking and which ones may cause an adverse reaction, Gary said. Losing access to that kind of information “adds to the complexity” of practicing medicine, he said.

System crashes leave providers without easy access to crucial information about their patients, so they have to find other ways to get the data, Gary said. Mostly this involves doing it the “old-fashioned way,” such as by asking patients and their families about their medical histories and recording them in paper-based records, he said.

Systems often include checklists for doctors and nurses. Without those lists, they have to go back to their training and think through the treatment process on their own, Gary said. Before EMRs were a thing, most doctors did this as a matter of

course. It was part of their “muscle memory,” Gary said. Doctors who have become overly reliant on technology to tell them “if A, then B,” may have difficulty adapting, he said.

An adverse medical event that occurs during a period when a system is down will be examined under a microscope, but won't necessarily result in liability for the hospital, Gary added. Computer systems are facilitators of treatment, they don't treat the patient, he said.

Clinicians are the care providers, so the question always will be whether the professional acted reasonably and in compliance with the standard of care, given the circumstances, Gary said.

Avoiding the ‘Perfect Storm’

There normally are several redundancies built into hospital computer systems in order to prevent a crash. These include recovery programs and cloud-based storage systems to stop the loss of or quickly restore access to critical information. If, however, “a perfect storm” occurs, and multiple, successive things go wrong, there could be a system shutdown, Gary said. There is no such thing as a failure-proof system, he said.

Hospitals can avoid or limit liability by creating hospital-wide backup systems that are tested and updated frequently to account for changing realities, Murphy said. Both the legal and compliance departments should be involved in developing a strategy to reassess the system periodically, she said.

An immediately accessible backup system, usually administered by the system's vendor or another outside source, is one way to avoid crash-created problems. But a smaller, less sophisticated hospital, may not have an effective crash-recovery system, David Adams, vice president of business intelligence and revenue cycle management at Crux Strategies, told Bloomberg Law.

Smaller hospitals may have fewer resources they can dedicate to ensuring their systems aren't vulnerable to a crash, Adams, who specializes in health-care technology, said. For example, a larger facility may have two or more points of entry for their internet connection, while a smaller system may have only one, leaving it more vulnerable if that connection goes down.

Larger institutions, on the other hand, generally have bigger systems with multiple interfaces, Murphy said. More moving parts, however, means there are more things that potentially can go wrong.

Responding to the Crash

Hospitals should develop enterprise-wide response plans that also are part of an integrated cybersecurity plan, Murphy said. The governing board, the hospital administration, the legal team, the compliance team, and the clinical staff should be involved in developing that plan, Murphy said.

The hospital's administration first should conduct a “robust” risk analysis, Murphy said. Then, with input from other departments, it should develop protocols and procedures to outline what will happen inside the hospital in the event of a system crash.

The multi-part contingency plan should include an emergency-mode operational plan. The hospital staff should be trained and periodically tested on that plan, Murphy said. She suggested hospitals run practice exercises that account for various scenarios, not unlike active shooter or workplace safety drills.

It is essential that the clinical staff understand how they should continue to operate during a system crash, Murphy added. The hospital thus should develop protocols for using paper-based records and secure mobile devices to collect and access clinical information. They also should have a procedure for entering information into EMRs once the system is back up, as well as for ensuring the information collected is secure.

A hospital's reaction to a crash will depend on the circumstances, Murphy noted. For example, the response to a crash expected to be of short duration will be different from one for which no end is in sight. Something expected to go on for days, for example, might lead the hospital to cancel elective procedures or divert some cases to another nearby facility.

It is hard to know what the precise response to a crash will be, Murphy said. But, before one happens, it is important to understand and assess the risk, develop a coherent multidisciplinary response, and deploy sufficient resources for response implementation.

To contact the reporter on this story: Mary Anne Pazanowski in Washington at mpazanowski@bloomberglaw.com

To contact the editor responsible for this story: Peyton M. Sturges at psturges@bloomberglaw.com

Notes

No Notepad Content Found