
— HOSPITAL LITIGATION

When the Screens Go Dark

Cyberattacks, EHR Downtime, and the Care That Happened Anyway

BY MICHELLE CARROLL · FOUNDER & CEO, LEXCURA SUMMIT

When people talk about healthcare cyberattacks, they usually start with stolen data and money. Those costs are real. The February 2024 ransomware attack on Change Healthcare disrupted claims and pharmacy operations across the country and ended up affecting an estimated 192.7 million people, the largest healthcare data breach on record. A few months later, a ransomware attack on Ascension pushed hospitals in several states onto paper and led to ambulance diversions.

A clinical review asks something else: what care did patients get while the systems were down, and what information did the people caring for them actually have? You shouldn't assume a tech outage proves care was bad. You also shouldn't assume it excuses it.

WHAT ORGANIZATIONS ARE SUPPOSED TO HAVE IN PLACE

Some of this is binding. The HIPAA Security Rule already requires a contingency plan, including data backup, disaster recovery, and an emergency mode operation plan (45 C.F.R. § 164.308(a)(7)). A proposed update published in January 2025 would add more specific requirements, including written procedures to restore certain systems and data within 72 hours. As of September 2026 it isn't final, and the federal regulatory agenda now targets 2027. CMS's emergency preparedness rule for hospitals requires an all-hazards plan that includes "a system of medical documentation that preserves patient information, protects confidentiality of patient information, and secures and maintains the availability of records" (42 C.F.R. § 482.15). And hospitals in Medicare's Promoting Interoperability program have to attest to an annual self-assessment using ONC's SAFER Guides. For 2026 that covers the full set of 2025 guides, including one on contingency planning for EHR downtime.

Some of it is voluntary. HHS's Cybersecurity Performance Goals, released in 2024, list "essential" and "enhanced" practices to help organizations decide what to do first, and the HHS 405(d) program's *Health Industry Cybersecurity Practices* does something similar. These are voluntary, and it's a mistake to describe every listed practice as a binding legal duty. Whether and how they bear on the standard of care in your jurisdiction is a question for counsel.

PIN DOWN WHAT WAS ACTUALLY DOWN

Picture a fictional hospital in a long outage. Some departments can still see old records. Others are charting on paper. The lab is still running tests, but results don't show up where they normally do. Staff are using workaround communication while IT tries to restore everything.

A patient comes in with several chronic illnesses and an incomplete medication history. Later, questions come up about a medication decision and a delay in acting on a lab result.

"The computers were down" is fine in conversation and useless in a case. Find out which systems were out: the EHR, order entry, pharmacy, the lab interface, imaging, bar-code scanning at the bedside, clinical messaging. Find out when each one went down and came back, whether it hit every department the same way, whether clinicians had a read-only downtime viewer, whether the lab could produce results the normal display couldn't show, and when downtime procedures were officially started, and by whom. Orders, medication records, imaging, and messaging may each have been affected differently, and the clinical consequences depend on which function failed and what replaced it.

The cause also needs evidence. Not every outage is an attack. Hardware failures, bad updates, and vendor problems cause downtime too. For the clinical review, the question is often the same whatever the cause: how did the team care for patients under the conditions it actually had? Figuring out who or what caused the outage is a separate investigation.

REBUILD CARE FROM THE PAPER

During downtime, the most important records may be outside the electronic chart entirely: paper orders, paper MARs, downtime census and tracking sheets, phone logs, photos of whiteboards, handwritten notes. Confirm they exist and were kept. Don't assume it.

An electronic export that looks oddly thin for the outage period may just reflect how people were charting, not a lack of care. The next step is finding the paper and learning how, and whether, it got into the permanent record. Some hospitals scan downtime paper into the EHR afterward, some re-enter it by hand, and some do both.

This is a Record Integrity question, the first pillar of the Lexcura Clinical Intelligence Model. You need to know whether the production includes the downtime sources, whether entries were transcribed later and by whom, whether a timestamp reflects when something happened or

when it was typed in afterward, and whether back-entered notes include things people only learned later.

If a dose is entered electronically the day after it was given, someone reading the chart without the paper MAR may put it at the wrong time. Timeline Reconstruction has to keep care time, charting time, and entry time visibly separate.

Watch for double entries after recovery, too. When a scanned paper record and a re-entered electronic record describe the same event, counting both makes it look like the patient got treated twice. Ignoring the paper throws away detail about what people knew at the time.

FOLLOW THE LAB RESULT

Back to the fictional patient. A critical potassium comes back through a workaround. The automatic alert isn't working. A lab tech calls the unit, but the call log entry is short. Treatment starts hours later.

Follow the result from the lab to the bedside. Who took the call, and were they responsible for this patient? What exactly was said, and was a read-back documented? With the electronic inbox down, who was watching for new results? How was that handled at shift change? And what happened next, and when? A log showing a call was made matters, but it doesn't necessarily finish the story. The Joint Commission's expectation that critical results be reported promptly (NPSG.02.03.01) doesn't take a break during downtime. Only the method changes.

Three kinds of records answer three different questions. The downtime plan shows what the organization meant to happen. Training and drill records show whether staff were ready to use it. The patient's records and the communications at the time show what actually happened for this patient. Don't assume the plan was followed to the letter.

The clinical significance still depends on the result and the patient. Some findings need action right away; others can safely wait. The review has to explain how urgent this result was for this patient and whether the delay changed the course of care.

MEDICATION SAFETY WITHOUT THE USUAL GUARDRAILS

Downtime takes away a lot of the electronic safety nets clinicians rely on: allergy checks, dose-range warnings, drug-interaction screening, and bar-code checks at the bedside. Look at what replaced them. Where did the medication history come from: the patient, family, an outside pharmacy, another facility? How were allergies confirmed? How did nurses know which order was current when paper and electronic records both existed? How was each dose charted so the next nurse knew what had already been given? Was pharmacy still verifying orders, and how?

If there was an adverse drug event, it needs its own analysis: the drug, the dose, the timing, the patient's own risk factors, and evidence of harm. "The outage increased risk" doesn't prove the outage caused this event.

There may also be evidence that people adapted well. A pharmacist tracks down an accurate list from an outside pharmacy, catches a discrepancy, and prevents an error. That belongs in the review. A disrupted hospital can have both real successes and real failures. Calling the unit "chaotic" conveys stress but tells an attorney almost nothing about the decision under review. Specific events make for a more useful analysis, and a fairer one.

RECOVERY HAS ITS OWN RISKS

Getting the systems back doesn't end the danger. Paper orders written during downtime can clash with stale electronic orders that come back to life on restoration. Results phoned in during the outage can later populate the chart, leaving staff to figure out whether anyone already acted on them. Results that never got communicated may only surface after recovery, sometimes days later. And back-entry can leave the electronic record incomplete for a while after everything's "back up."

Suppose the team restores access and follows an old electronic medication order without realizing a paper order changed it during the outage. That's a reconciliation failure, a different mechanism from an error made while the systems were down. A review that stops at the restoration time will miss it. For counsel, the relevant window may run well past the outage itself, until the disputed information was reconciled, acted on, or otherwise resolved.

KEEP THE QUESTIONS IN THEIR LANES

These cases can raise organizational, technical, and clinical questions all at once, and each needs different expertise. A clinical reviewer can judge whether bedside care was reasonable under the conditions that existed. Whether the security setup met technical expectations is a question for a different expert. And the legal weight of a policy, a voluntary framework, a contract, or a regulation is for counsel.

What the clinical side contributes is how the outage collided with this patient's needs: which decision depended on information nobody could see, what alternative was realistic under the circumstances, what staff actually did, and what evidence supports or undercuts the link to the outcome.

A fair review doesn't judge clinicians as if they had normal electronic access when they didn't. It looks at the reasonable options they actually had, while still asking whether the organization's preparation and response supported safe care.

RECORDS WORTH REQUESTING

- The downtime incident timeline, including when downtime procedures started and ended, by system and department
- The downtime and contingency plans, and the emergency preparedness plan, in effect at the time
- Paper downtime records: orders, MARs, census and tracking sheets, lab call logs, communication logs
- Records of how and when paper was scanned or re-entered, with audit data for re-entered entries
- Downtime training and drill records for the units involved
- SAFER Guide self-assessments, especially contingency planning, where discoverable
- Post-incident reviews, root cause analyses, and after-action reports (privilege rules vary)

The most productive request you can make is for a review that identifies each specific clinical problem, whether a delayed result, an unresolved medication conflict, or an imaging study nobody could see, and explains each one on its own before pulling them together. When the technology fails, follow the patient's care through the workaround and into recovery. That's where the record shows how the organization's response played out for one patient.

SOURCES

- HHS, *Healthcare and Public Health Sector-Specific Cybersecurity Performance Goals*
- ASTP/ONC, *2025 SAFER Guide: Contingency Planning*
- 45 C.F.R. § 164.308(a)(7); HHS/OCR, *HIPAA Security Rule To Strengthen the Cybersecurity of Electronic Protected Health Information*, proposed rule, 90 Fed. Reg. 898 (Jan. 6, 2025)
- 42 C.F.R. § 482.15
- CMS, Medicare Promoting Interoperability Program, SAFER Guides measure
- HIPAA Journal, *Largest Healthcare Data Breaches* (Change Healthcare, 192.7 million individuals)

This newsletter is for education only and isn't medical, legal, or technical security advice. The case is fictional. Regulatory status reflects sources reviewed in September 2026.

ABOUT LEXCURA CLINICAL INTELLIGENCE

Lexcura Clinical Intelligence provides integrated clinical and regulatory analysis for attorneys handling healthcare litigation. If you have a case where care happened during an EHR outage or cyberattack and want it rebuilt from the paper records through recovery, we'd welcome the conversation.

Michelle Carroll

FOUNDER & CEO, LEXCURA SUMMIT

