Letter to the Editor

Unplugged and Overwhelmed: The New Reality of Medical Training

Amber Hernandez, BS[1]; Ariel P. Santos, MD, MPH, FRCSC, FACS, FCCM[1]

Introduction

A typical morning for a surgical resident begins with logging into the electronic medical record (EMR) to extract patient information in preparation for rounds and before heading to the operating room. It is a critical platform that residents have become reliant on. But what happens when this system goes dark? Not for minutes, but for days, weeks, or even months.

Cyberattacks on healthcare institutions are escalating. It is no longer hypothetical. If you personally haven't been a part of a system that has been attacked, then you are probably aware of other healthcare institutions that have fallen

victim. Ransomware attacks on US hospitals more than doubled from 43 to 91 annually between 2016 and 2021, with 44% causing operational disruptions including electronic system downtime.[1] When one academic Level 1 trauma center experienced a 25-day total EMR downtime following a cyberattack, operative time decreased by 53%.[2] However, while literature primarily focuses on the operational and financial impacts of cyberattacks, a critical question remains unaddressed. In September 2024, our own institution at Texas Tech University Health Sciences Center experienced a cyberattack, reinforcing the urgency of this issue. This is a patient safety crisis. Surgical residents prepare for many things, but how much of their training consists of how to safely and effectively treat patients while experiencing EMR downtime?

The Training Gap

The transition from paper to electronic records has created a world where the next generation of physicians have primarily never practiced medicine without digital support. Through our own experience, it was surprising to discover the inexperience residents had in writing medical notes without a standardized online template. One institution agreed that it is critical to warn other institutions that residents need to understand everything down to the basics, even things as simple as using black ink and drawing a single line through errors.[3] Most residents graduate medical school with very little training on a paper-based system, and they must understand what to do when the EMR fails them.

This deficit extends beyond basic documentation. Surgical residents must manage complex perioperative workflows. They are responsible for tracking laboratory values, managing drains and lines, adjusting medications, and ensuring seamless handoffs between teams. In the digital era, these tasks are mitigated using the EMR. During downtime, these tasks can be disrupted, posing issues in the provision of clinical care and causing patient safety issues.

To put things into perspective, season 2 episode 8 of The Pitt offers a clear example of how a cyberattack can disrupt patient care in real time. While there were things that worked, many of the challenges arose from a lack of prior hands-on training, in which things could have run more smoothly. The hospital administration and department heads clearly had a cyberattack plan in place; however, the staff that keeps the hospital running were not properly prepared for

Corresponding Author:
Amber Hernandez, BS
Texas Tech University Health Sciences Center School of Medicine, Lubbock, TX
Email: amber00132@gmail.com

the situation. Staff were trained on the spot, leading to confusion and unclear expectations.[4] This highlights a critical gap between having a plan and being able to implement it.

The 2024 CrowdStrike outage, caused by a faulty software update, led to widespread system failures across many health care institutions. It demonstrated that even benign causes of EMR downtime can significantly impact patient care.[5] Healthcare systems are not only vulnerable to attack, but also unexpected technological failure.

Impact on Surgery

Surgery is uniquely vulnerable to EMR downtime. Unlike outpatient clinics that can reschedule appointments, patients coming in with trauma, emergent surgical conditions, and those who are critically ill must be attended to expediently. Reports of prolonged EMR outages in perioperative settings describe disruptions ranging from operating room scheduling to failures in patient identification, each posing risks to patient safety.[6] During the 25-day cyberattack at an academic trauma center, the dramatic reduction in operative capacity was attributed to multiple factors, but the role of resident preparedness was never examined.[2] How much of that 53% decrease in operative time resulted from residents struggling with unfamiliar paper workflows?

Consider the large realm of tasks a surgical resident must complete for a single postoperative patient without EMR access. The list is endless. They must handwrite admission orders, manually track intake and output, communicate lab results verbally rather than automated alerts, write legible operative notes that other teams can interpret, and coordinate care transitions without electronic handoff tools. Each step introduces opportunities for error when residents lack experience with manual workflows.

A Call to Action

It is crucial for residency programs to take action with structured steps to ensure residents can safely deliver care without an EMR. Programs should consider implementing a structured EMR downtime preparedness training into their curriculum. This is about patient safety and systems-based practice, which are part of the core competencies of the Accreditation Council for Graduate Medical Education (ACGME).

First, programs should implement simulation-based downtime training. Residents should participate in structured exercises that replicate prolonged EMR outages, requiring them to write admission orders, document operative notes, track laboratory data, and coordinate care using paper-based systems. These simulations should reflect real-world complexity. Simulation training allows residents to perform routine clinical tasks without reliance on the EMR, serving both as a teaching tool and a systems test. This training not only helps residents develop competence in paper-based systems but also reveals institutional weaknesses in contingency planning when protocols are put into action.[7] One study evaluated surgical residents completing a simulation several weeks after a didactic session and found that participants reported improved skills and greater confidence in managing adverse scenarios. [8] Demonstrating that even one review can establish confidence in putting paper-based systems to use. Although some may argue this adds to an already demanding training burden in residency, this does not have to be a time-consuming preparation. Even brief instruction on expectations for paper-based documentation can provide meaningful benefit.[8,9]

Second, competency in fundamental paper-based workflows should be established as a core training expectation. Residents should demonstrate the ability to write clear orders, maintain accurate patient lists, track intake and output, and perform safe handoffs without reliance on electronic tools. Simple structured systems can support this, such as placing clipboards at each bedside with updated labs, vital signs, intake and output, along with a communication chart in each room to keep providers and adjunct services aware of ongoing tasks. These are not outdated skills, but essential safeguards during system failures.

Third, institutions should incorporate residents and medical students into downtime

preparedness planning. Residents are frontline providers during these events. Defining resident roles, communication pathways, and escalation processes during EMR outages is critical to maintaining continuity of care. As demonstrated in The Pitt, having a plan in place is not enough if frontline staff are unfamiliar with how to execute it in real time.[4] Incorporating all members of the care team, including residents, into preparedness planning ensures that protocols are usable in practice. Communication between teams and staff is essential; it is a crucial part of downtime preparedness. The procedures for communication should not only be planned but also be practiced.[10]

Finally, downtime preparedness should be standardized throughout the institution. When unexpected EMR downtime occurs, there should be standardized procedures for all residents to follow. This should include providing standardized templates for writing orders, notes, and prescriptions with examples to eliminate any confusion on expectations.[3] These paper-based templates should be regularly refined based on real-world use to improve efficiency when implemented.[11]It is also recommended to establish a meeting point, such as the chief medical resident office, to create a primary place where residents can receive updates and written templates.[3] Additionally, the use of whiteboards for tracking patients and maintaining updated patient lists, along with alternative communication methods such as faxing information to lab and radiology, can help maintain workflow during downtime.

Conclusion

As a medical student applying to general surgery residency, I recognize that my generation has grown up with technology as an extension of our clinical practice. But technology is a tool, not a replacement. When that tool fails, we must be prepared to deliver safe and effective surgical care using whatever systems remain available. The increasing reliance on the EMR has created a vulnerability that needs to be protected. Current residency education does not adequately prepare residents to function safely during EMR downtime, putting clinical workflow, communication, and patient care at risk.

Direct evidence from real-world downtime events and illustrative scenarios, such as those from The Pitt, demonstrates that even when institutional plans exist, patient care can be compromised if staff on the frontline are not adequately trained to execute them. Delays in care, miscommunication, and unclear roles are not only inconvenient but also a threat to patient safety.

The next cyberattack is not hypothetical. As healthcare systems invest in technological defenses, equal attention must be given to preparing the physicians who will deliver care when those systems fail. Cyberattacks are becoming more common; the downtime is disruptive, and residents lack experience with paper-based workflows. What remains missing is action. This gap in training is both identifiable and correctable. Surgical education must evolve to address this gap before the next ransomware attack causes preventable patient harm. Residents should be prepared to deliver safe and effective care no matter the EMR system availability. Without deliberate action, we risk placing both residents and patients in preventable danger during the next inevitable cyberattack. As with most things in medicine, an ounce of prevention is worth more than a pound of cure.

References

1. Neprash HT, McGlave CC, Cross DA, et al. Trends in Ransomware Attacks on US Hospitals, Clinics, and Other Health Care Delivery Organizations, 2016-2021. JAMA Health Forum. 2022;3(12):e224873. doi:10.1001/jamahealthforum.2022.4873
2. Tarka M, Blankstein M, Schottel P. The crippling effects of a cyberattack at an academic level 1 trauma center: An orthopedic perspective. Injury. 2023 Apr;54(4):1095-1101. doi: 10.1016/j.injury.2023.02.022. Epub 2023 Feb 10. PMID: 36801172.
3. Paul C, Bilger E, Kango G, Reyes JA, Catalanotti JS. Residency Program Preparedness for Prolonged Downtime: Lessons Learned From a Cyberattack. J Grad Med Educ. 2021 Oct;13(5):626-630. doi: 10.4300/JGME-D-21-00253.1. Epub

2021 Oct 15. PMID: 34721788; PMCID: PMC8527927.
4. "2:00 PM." In: The Pitt. Season 2, Episode 8. HBO Max; 2026
5. Tully JL, Rao S, Straw I, Gabriel RA, Longhurst CA, Savage S, Voelker GM, Dameff CJ. Patient Care Technology Disruptions Associated With the CrowdStrike Outage. JAMA Netw Open. 2025 Jul 1;8(7):e2530226. doi: 10.1001/jamanetworkopen.2025.30226. Erratum in: JAMA Netw Open. 2025 Aug 1;8(8):e2531871. doi: 10.1001/jamanetworkopen.2025.31871. PMID: 40682764; PMCID: PMC12276631.
6. Cheon EC, Shaffer S, McCarthy K, Leavitt O, Mukerji S, Hardy C. Continuing Anesthesia Services in the Face of a Prolonged Digital Health System Outage. Anesthesiology. 2025 Aug 1;143(2):266-274. doi: 10.1097/ALN.0000000000005508. Epub 2025 Jun 10. PMID: 40493406.
7. Abbou B, Kessel B, Ben Natan M, Gabbay-Benziv R, Dahan Shriki D, Ophir A, Goldschmid N, Klein A, Roguin A, Dudkiewicz M. When all computers shut down: the clinical impact of a major cyber-attack on a general hospital. Front Digit Health. 2024 Feb 16;6:1321485. doi: 10.3389/fdgth.2024.1321485. PMID: 38433989; PMCID: PMC10904636.
8. Nguyen N, Watson WD, Dominguez E. Simulation-Based Communication Training for General Surgery and Obstetrics and Gynecology Residents. J Surg Educ. 2019 May-Jun;76(3):856-863. doi: 10.1016/j.jsurg.2018.10.014. Epub 2019 Feb 28. PMID: 30826262.
9. Zhao JY, Kessler EG, Yu J, Jalal K, Cooper CA, Brewer JJ, Schwaitzberg SD, Guo WA. Impact of Trauma Hospital Ransomware Attack on Surgical Residency Training. J Surg Res. 2018 Dec;232:389-397. doi: 10.1016/j.jss.2018.06.072. Epub 2018 Jul 19. PMID: 30463746.
10. Stowman AM, Cacciatore LS, Cortright V, McConnell J, Wilburn C, Bryant B, Frisch N, Kalof AN. Anatomy of a Cyberattack: Part 3: Coordination in Crisis, Development of an Incident Command Team, and Resident Education During Downtime. Am J Clin Pathol. 2022 Jun 7;157(6):814-822. doi: 10.1093/ajcp/aqab162. PMID: 35188562.
11. Larsen E, Fong A, Wernz C, Ratwani RM. Implications of electronic health record downtime: an analysis of patient safety event reports. J Am Med Inform Assoc. 2018 Feb 1;25(2):187-191. doi: 10.1093/jamia/ocx057. PMID: 28575417; PMCID: PMC7647128.

Affiliations:
[1]Texas Tech University Health Sciences Center, School of Medicine, Lubbock, TX