JAMA Network Open

Original Investigation | Health Informatics

Patient Care Technology Disruptions Associated With the CrowdStrike Outage

Jeffrey L. Tully, MD; Sumanth Rao, MS; Isabel Straw, BMBS, PhD; Rodney A. Gabriel, MD, MAS; Chris Longhurst, MD, MS; Stefan Savage, PhD; Geoffrey M. Voelker, PhD; Christian J. Dameff, MD, MS

Abstract

IMPORTANCE Modern health care depends on digital infrastructure. Widespread technology outages affecting health care delivery organizations may impact clinical care.

OBJECTIVE To determine the availability of health care delivery organization internet-connected networks before, during, and after the faulty CrowdStrike software update of July 19, 2024.

DESIGN, SETTING, AND PARTICIPANTS This cross-sectional study measured availability of health care delivery organization networks by performing scans on internet address ranges and Fast Healthcare Interoperability Resources (FHIR) end points corresponding to individual hospitals, spanning various sizes, geographic range, and organizational types, assessing responsivity to scans 2 weeks before, during, and 2 weeks after the CrowdStrike update. Hospitals affiliated with US-based health care delivery organizations that used the Epic electronic health record and that had publicly observable internet services, including FHIR end points, were included. Data were analyzed from July 19, 2024, to May 17, 2025.

EXPOSURE A widely distributed faulty software update for enterprise cybersecurity software distributed on July 19, 2024, which, when installed on computers, resulted in a system crash.

MAIN OUTCOMES AND MEASURES The primary outcome was loss of response to internet scanning techniques indicating computer system downtime. A secondary analysis was performed on unresponsive domains attempting to identify the function of the network services provided.

RESULTS Among 2232 hospitals with available data, loss of response to internet scanning techniques immediately following the CrowdStrike update was observed in 759 hospitals (34.0%). A total of 1098 distinct network services with outages were identified, of which 631 (57.5%) were unable to be classified, 239 (21.8%) were direct patient-facing services, 169 (15.4%) were operationally relevant services, and 58 (5.3%) were research-related services.

CONCLUSIONS AND RELEVANCE This cross-sectional study of US hospitals found that a widespread technology outage was associated with outages in patient-facing network services integral to care delivery. These findings suggest that internet measurement techniques may be useful for surveillance and study of critical digital health care infrastructure.

JAMA Network Open. 2025;8(7):e2530226. doi:10.1001/jamanetworkopen.2025.30226

Key Points

Question What patient care outcomes were associated with a major international technology outage?

Findings In this cross-sectional study of 2232 hospitals with available data, network disruptions coinciding with a faulty cyber security software update on July 19, 2024, were measured at 759 US hospitals. Of the nearly 1100 internet-based services examined, 239 (21.8%) were characterized as corresponding with direct patient care functionality.

Meaning These findings suggest that widespread technology failures affecting health care infrastructure may have commensurate negative impacts on patient care systems.

+ Supplemental content

Author affiliations and article information are listed at the end of this article.

Introduction

Modern health care delivery depends on an increasingly complex digital infrastructure. The physician using an electronic health record (EHR), ordering and reviewing laboratory and radiographic studies, or capturing charges for subsequent reimbursement likely relies on a network of computers running software, connected to the wider internet, to care for patients.

This shift has brought improvements in the quality and efficiency of care but has also created a new source of risk.[1-4] Examples of technology failures, both inadvertent and intentional, resulting in the disruption of patient care have proliferated in recent years.[5-9] Independent of etiology, loss of critical systems often necessitates the use of downtime procedures, which are frequently underprepared for and are associated with increased likelihood of medical error.[10-12] While the initial impact of an innocuous event, like a power failure, may result in the same need for downtime procedures as a targeted cybersecurity incident, the ultimate duration and scale of the disruptions may vary widely.[13]

Although cybersecurity incidents are an increasingly prominent source of technology failures, nonmalicious events, including unplanned network outages, failures in key infrastructure services, and software failures, can be equally disruptive. In particular, automated software updates, while critical to improving the function or security of systems, can result in widespread crashes if the update itself is faulty. Such outages have been documented with updates to EHR software, as well as with nonclinical software widely deployed in enterprises across many sectors.[14-17]

One such outage was recently associated with CrowdStrike, a cybersecurity software company, whose Falcon software is designed to monitor and protect computers of large commercial enterprises from cybersecurity threats. On July 19, 2024, a faulty update for Falcon was simultaneously distributed via the internet to millions of personal computers and servers running certain versions of the Windows operating system (Microsoft) and the Falcon software.

The update contained a programming error that caused computers that installed the update to reboot and crash. Installing the repair or patch for this update required direct manual access to each affected computer and could not be accomplished remotely through the internet—a time-intensive and laborious process resulting in downtimes of hours or even days for many organizations.[18,19]

The impact from the Falcon update outage was immediate and global.[20] Disruptions were sustained across dozens of industries in dozens of countries: air travel saw the cancellation of thousands of flights worldwide, large banks and federal government systems in the US were impacted, and some factories and ports briefly shut down.[21] Few sectors were spared, and health care was no exception, with large academic centers reporting an inability to access EHRs and the cancellation of elective surgeries.[22] Emergency response services across multiple countries were adversely affected, and several of the largest laboratory vendors in the US had delays or were unable to process results.[23,24]

Today there is no public health surveillance system that monitors the well-being of critical health care technology systems. However, because such systems are part of a larger global internet infrastructure, their failures are frequently reflected in symptoms visible via the public internet. Indeed, a large body of existing research in applied computer science has developed techniques to infer and characterize various kinds of system failures based entirely on the results of diligent and focused internet measurements.[25-28] Variants of these same techniques, when applied and specialized to hospital infrastructure, show promise in monitoring and quantifying disruptions to critical digital health care technology. We report the development of a system to monitor and detect disruptions in critical digital health care infrastructure.

Methods

This cross-sectional study was deemed exempt from institutional review board review and informed consent by the University of California, San Diego, as this study had no human participants. This study is reported following the Strengthening the Reporting of Observational Studies in Epidemiology (STROBE) reporting guideline.[29]

Study Design

This cross-sectional study was conducted between July 5, 2024, and August 3, 2024. Data for 2 weeks before (July 5-18), during (July 19), and after (July 20 to August 3) the CrowdStrike outage

were collected and analyzed. US health care delivery organizations (HDOs) running Epic EHR software (Epic Systems) that had at least 1 publicly available Fast Healthcare Interoperability Resources (FHIR; The HL7 FHIR Foundation) internet end point were included.

Data Sources

Data for this study were collected as part of a preexisting initiative to prospectively monitor hospital ransomware attacks with funding from the Advanced Research Projects Agency for Health. We collected and cataloged internet address ranges for HDOs and hospitals that use Epic as their EHR provider and that host external and public-facing internet services. We used a provider of historical internet measurement data (Censys), to match hospital domains to Internet Protocol (IP) ranges, filtering using Domain Name System and x.509 certificate information provided by Censys's daily snapshot of the internet address space. Services running on the identified hosts were similarly enumerated. FHIR end points were identified from public data, including the Lantern Project,[30] a publicly available resource from MITRE.

Data Collection

Hospital IP range scans were performed using an open-source tool designed to probe open network ports of internet-connected hosts (ZMap version 4.2.0; University of Michigan).[31] Address ranges were probed in rounds of 3 hours, and a positive scan (on any port) indicated an online host end point. Scans of FHIR end points were performed in rounds of 2.5 hours using a Python (Python Software Foundation) hypertext transfer protocol client. Positive scan results, ie, end point was operational and communicating with outside internet traffic, as well as negative scans, ie, system downtime, were recorded and stored on a secure internal server.

Downtime Classification

Downtime for the address range scans was defined as the period between when a deviation from the normative count of positive IP scans (by a factor $\geq$2 SD) occurred to when it recovered. Downtime for a hospital or HDO was defined as the maximum downtime for any network on which it hosted any service.

Downtime for the FHIR end point scans was defined as the time between a negative scan and the return of a positive scan. End points in our list that had no positive scan the entire duration of the study were excluded. Downtime instances were then collated into a dataset for subsequent analysis of potential clinical effects.

Clinical Translation

Once unresponsive network services were identified, further steps were taken to provide a clinical interpretation of the services related to each HDO or hospital to infer potential impacts on clinical operations. Four researchers independently analyzed 1098 affected services in the CrowdStrike outage dataset. The clinical relevance of the 1098 affected services was investigated through (1) directly visiting site Uniform Resource Locators (URLs), (2) Google dorking, a technique harnessing search engines to identify specific text in website code,[32] and (3) Domain Name Service evaluation through terminal queries.[33] Where further confirmation was needed, Client for URL requests were used to check site availability, hypertext transfer protocol status codes, and headers to attempt to determine the clinical function of an IT service. Viewing the page source provided additional insights, such as metadata with information on the services behind a login portal (eg, remote staff access portals for patient records) and hidden redirects.

Through the combination of these methods, each affected service was manually assigned a label detailing its function within clinical operations (eg, patient portal for health care record). Examples of each method and successfully identified results were collected and are provided in the eTable in Supplement 1. Based on the manual labels, each service was assigned 1 of 4 categories capturing its relevance to patient care: (1) patient facing (eg, radiological imaging systems), (2)

operationally relevant (eg, staff scheduling systems), (3) research relevant (eg, research databases for clinical trial operations) and (4) not relevant or unknown (eg, donation pages for academic institutions). For categories 1 to 3, the service had to affect patient experience; thus, services such as research laboratory information webpages were excluded and placed in category 4. Services that could not be identified due to internal network or security restrictions or that were decommissioned and unavailable were also placed in category 4.

Statistical Analysis

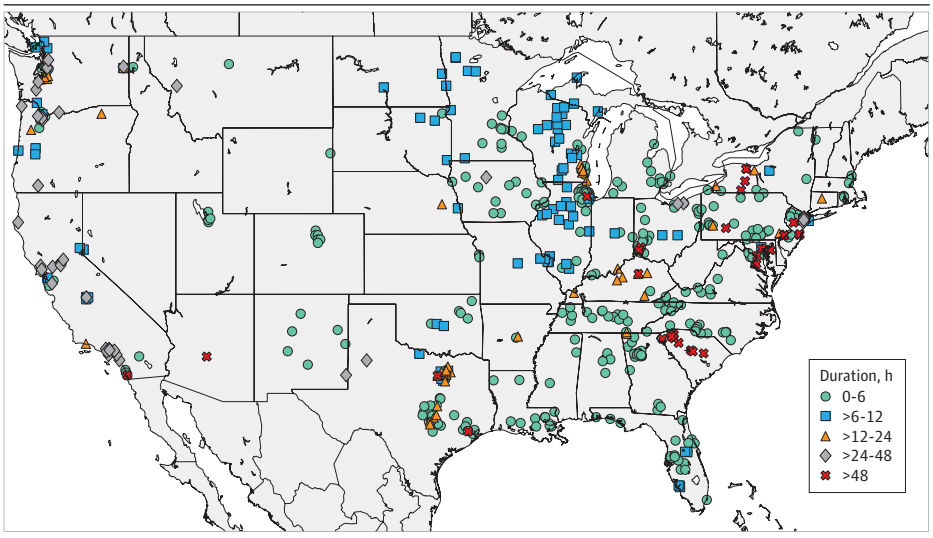
A deviation-from-baseline was established using a trailing 2-week window of 112 scans (8 hours per day × 14 days) of unique IP counts per hospital. Downtime events were flagged during the study period when the deviation met or exceeded 2 SD. This approach allowed consistent thresholds across institutions. For FHIR end points, we performed 2 comparisons using *t* tests. A 1-sample *t* test was used to determine whether the event count on the incident day represented a statistically significant outlier. A Welch 2-sample *t* test was used to compare the mean daily event counts between the preincident and postincident groups to account for potentially unequal variances between groups. A 2-sided $P < .05$ was considered statistically significant. As this is an observational study, corrections for multiple comparisons were not applied; instead, emphasis on clinical or infrastructural effects of disruptions was used in interpreting significance. Data were analyzed using Python version 3.12.8 (Python Software Foundation) from July 19, 2024, to May 17, 2025.

Results

Immediately following the CrowdStrike update on July 19, 2024, a total of 759 of 2232 hospitals with available data (34.0%) experienced service disruptions detectable with our methods. These disruptions were identified solely by IP address space scans in 460 hospitals (60.6%), solely by FHIR end point scans in 206 hospitals (27.1%), and by both methods in 93 hospitals (12.3%).

Further examination of affected domains across the hospitals yielded a total of 1098 individual disrupted digital services that were investigated for clinical relevance (eTable in Supplement 1). **Figure 1** provides a more granular illustration of this downtime duration across the country. Most hospital services recovered within 6 hours (321 services [29.2%]), with a smaller number of hospitals (43 services [3.9%]) experiencing outages of more than 48 hours (Figure 1).

Figure 1. Geospatial Map of the Identified Health Care Delivery Organizations Inferred to Have Service Disruptions Using Address Space Scans



Data points are color coded by the time to recovery following the CrowdStrike incident.

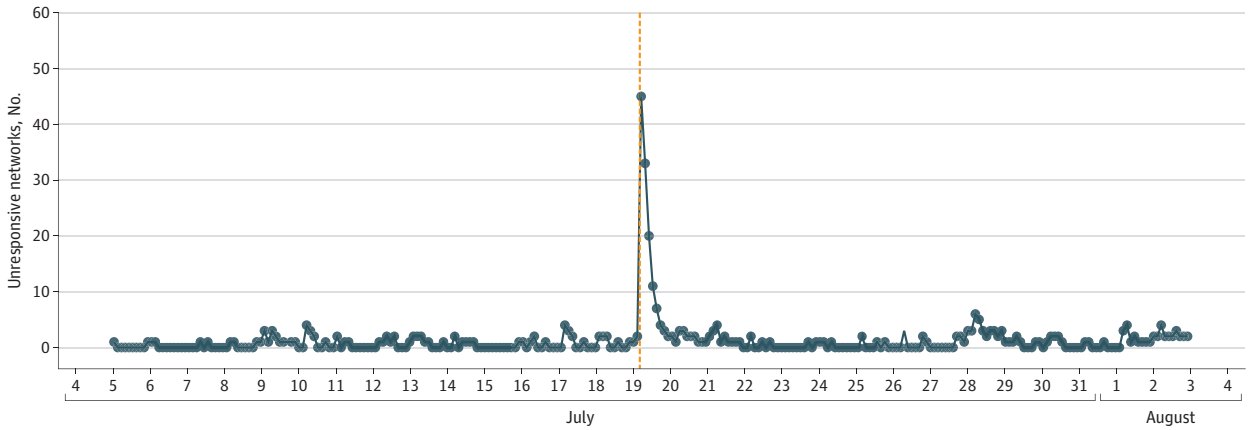
We also observed that a set of 52 unique HDOs (representing 299 individual hospitals) failed to respond to our FHIR scans immediately following the July 19 update. The change in FHIR outage detection occurring during the CrowdStrike event is presented in **Figure 2**, which displays unresponsive HDO Epic FHIR end points resulting from scans conducted 2 weeks before and 2 weeks after the CrowdStrike outage.

The mean (SD) daily FHIR end point downtime was significantly increased during the CrowdStrike incident compared with the pre-event and postevent periods, with 6.0 (3.7) events prior, 128 events during, and 10.5 (9.1) events after the CrowdStrike incident ($P < .001$). There was no significant difference in the means between the pre-event and postevent periods. The median (IQR) observed downtime for all HDOs during the event was 5.1 (2.5-8.1) hours, with most HDOs recovering within 5 hours (31 of 52 HDOs [59.6%]).

Outages in Clinical Systems

Of 1098 service outages, 239 (21.8%) were found to be patient facing, 169 (15.4%) were operationally relevant, 58 (5.3%) were research relevant, and 631 (57.5%) were not relevant or unknown (**Table**). Patient-facing services spanned imaging platforms, prehospital medicine health record systems, patient transfer portals, access to secure documentation, and staff portals for viewing patient details (Table). In addition to staff portals, we saw outages in patient access platforms across diverse hospital systems; these platforms, when operating as usual, allow patients

Figure 2. Unresponsive Health Care Delivery Organization (HDO) Fast Healthcare Interoperability Resource End Points Prior, During, and After the CrowdStrike Outage



The vertical orange line marks the time point at which the CrowdStrike outage occurred, July 19, 2024.

Table. Evaluation of Services With Outages and Their Relevant Clinical Utility

	Category of service			
	Patient facing	Operationally relevant	Research relevant	Not relevant / Unknown
Proportion of total affected services, No. (%) (n = 1098)	239 (21.8)	169 (15.4)	58 (5.3)	631 (57.5)
Examples of identified services and relevance to patient care	Staff portals for viewing patient health records, access to platforms for viewing prehospital clinical information, fetal monitoring systems and device management for telemonitoring, secure document transfer for inter-hospital transfers, access to imaging systems for viewing patient scans	Staff scheduling systems for regular and on call shifts, bill payment systems for health care insurers, clinical workforce management and optimization systems, portal for ordering facilities services, networked printers in the clinical environment, digital systems for establishing patient wait times and patient flow in the hospital environment	Access to databases for clinical trial operations, information websites for research laboratories, patient enrollment systems for rare disease research programs, staff login for clinical research management systems, REDCap research environment for academic centers, login portal for researchers at academic health centers	Testing and staging environments (preproduction), webpage for medical school alumni programs, donation websites for academic centers, medical education websites for students

to schedule appointments, contact health care practitioners, access laboratory results, and refill prescriptions. The not relevant or unknown category encompassed testing and staging environments for software that were in predeployment phases, donation pages for institutions, information pages on educational services, and educational resources for students (eg, medical and nursing students) (Table). The eTable in Supplement 1 provides further examples of successfully identified clinical services from the CrowdStrike outage dataset, with extracts of informative sections of source code, headers, and webpage details.

Discussion

In this cross-sectional study, we present a method of proactively monitoring digital signals corresponding to HDOs using well-established internet measurement techniques and report associated downtimes occurring at IP addresses corresponding to 759 hospitals during the CrowdStrike outage of 2024. To our knowledge, our data provide the first quantifiable insight into specific outcomes associated with this event. Our system measured disruptions in nearly 1100 unique services belonging to HDOs across the country. While most services (631 services [58.5%]) were either associated with nonclinical elements or unable to be categorized, characterization of the remaining elements allows for the most granular description of health care infrastructure outcomes associated with the CrowdStrike outage to our knowledge.

As digital systems are increasingly important element of health care infrastructure, technology failures can disrupt the delivery of care and increase risk to patient safety.[34-40] Technology failures that affect a widely used system, such as the CrowdStrike Falcon program, or a cyberattack on a company serving a large market share of HDOs, like the ransomware attack on Change Healthcare, can cause disruption on a national scale.[41] Information on the extent of impact, the locations of HDOs affected, and the types of patients most at risk when technology fails is often lacking or parceled out anecdotally in media reports. To our knowledge, no federal, regional, state, commercial, or trade association health care stakeholder or entity possesses the capability to assess in near–real time digital signals corresponding to the availability of national health care infrastructure technology.

A vast number of nonclinical systems are needed to sustain hospital operations, and outages were observed in critical logistics, human resources, and physical infrastructure during the CrowdStrike outage. Email applications, online staff schedules, productivity and project management tools, security cameras, payroll systems, physician credentialing software, remote access tools, virtual private networks, and cybersecurity controls were among the operationally relevant system outages observed, representing 15% of our dataset. Loss of these systems may indirectly affect patient care by exacerbating staffing shortages, degrading communication, preventing remote work, or increasing physical or cybersecurity vulnerabilities, and the disabled documentation and charge capture systems measured likely resulted in parallel challenges with clinical billing.

Among services with outages, 5% corresponded to clinical research enterprises. Specific tools, like REDCap (Vanderbilt) software used to create research databases, were inaccessible at some hospitals, and services belonging to identifiable, specific research laboratories studying immunology, oncology, epigenetics, environmental toxicology, and microbiomics experienced outages. Most concerning, clinical trial websites directly serving patients, as well as public health and regional registries used for tracking trauma, stroke, cardiac, and burn patients, suffered downtime.

Finally, we characterized 239 services (21.8%) whose outages may have had direct patient safety implications. A substantial number of hospitals lost important services involving their EHR, likely preventing physicians from accessing critical patient information, using automated ordering or clinical decision support, or easily viewing laboratory or radiology results. Similarly, externally facing patient health portals were disrupted, threatening to deprive patients access to their medical records, including new results or diagnoses, obstructing the ability to easily communicate with their clinicians or to be reminded about upcoming appointments and potentially even delaying care by

obfuscating critical paperwork or authorizations. Services belonging to websites used by hospitals to provide patient education, such as websites containing important information and instructions for expectant mothers, appointment help for parents seeking neuropsychological testing for their children, and occupational health resources for employees, were also found to be down.

Foundational critical software platforms, including Picture Archiving and Communications Systems and Laboratory Information System, were disrupted at some hospitals, potentially impacting critical clinical workflows dependent on the rapid results of imaging and laboratory studies. A number of patient monitoring systems, including fetal monitors, cardiac telemetry systems, and behavioral health applications, experienced outages, which may have had regional effects on some clinical applications, like prehospital reporting and telemedicine systems used to deliver care across distance, during the disruptions.

Public health surveillance systems have been long established as effective and critical for the monitoring of acute and long-term epidemiologic phenomena, from infectious disease outbreaks to toxic exposures to maternal and child health outcomes, and have been implemented on scales ranging from a single community to global views.[42-47] Similarly, the disciplines of disaster medicine and emergency incident response are predicated on the ability to collect data during and after disasters to analyze impact and develop future preparedness plans.[48-51] Visibility and insight into the normal and abnormal state of digital health infrastructure is thus a requirement in seeking to understand the increasingly complex relationships between technology and the delivery of patient care and to meaningfully characterize the effects of technology failure. As approaches to monitor digital health infrastructures evolve, the information they produce may become useful for stakeholders charged with preparing for and responding to public health or infrastructure-related emergencies, helping to identify geographic regions, patient populations, or classes of services most likely to be impacted during a technology failure, allowing for targeted intervention designed to minimize harm.

Limitations

This study has some limitations, and additional studies to develop these techniques are needed. Our method does not represent the definitive approach to obtaining comprehensive visibility of digital health care infrastructure, and limitations of this study include both classic problems in empirical internet measurement as well as challenges unique to health care delivery. The question of ground truth is inherent to a field where elements being measured are surrogates for the systems of interest. While downtime of an IP address corresponding to an EHR application programming interface strongly suggests disruption in the ability to use that EHR, without confirmation from clinicians at that institution, it is impossible to preclude a situation in which internal mitigations somehow enabled persistence of the underlying system. Similarly, while evidence exists to demonstrate that unplanned loss of clinical systems resulting in the transition to downtime procedures is associated with increase risk of error and decreased efficiency, generalizable clinical outcome data associated with such downtimes is correspondingly lacking. Technical considerations and limitations additionally give rise to seemingly arbitrary elements, such as the 2.5-hour scanning interval of the system and the fact that data are largely derived from health systems running the Epic EHR. Cloud-hosted digital services and those running behind firewalls are more challenging to measure with the approaches described; therefore, HDOs with less technically sophisticated networks and technology stacks may be overrepresented in these data. The development of further methods to allow for increased visibility into cloud dependencies and less publicly facing services is an area for future work. Large language models and other artificial intelligence tools may assist in identifying services and their associated functions at scale and with potentially increased accuracy.

Conclusions

This cross-sectional study found an association between the 2024 CrowdStrike outage and many geographically diverse HDOs experiencing significant technical system downtime. Hospital recovery

from the downtime was temporally varied. Prospective internet availability scanning of critical digital health care may serve as an early warning signal for adverse events, such as ransomware attack, data center failure, or faulty software, and could serve an important public health function as health care continues expanding its dependence on digital technology.

ARTICLE INFORMATION

Accepted for Publication: July 9, 2025.

Published: July 19, 2025. doi:10.1001/jamanetworkopen.2025.30226

Corresponding Author: Jeffrey L. Tully, MD, Center for Healthcare Cybersecurity, University of California, 9500 Gilman Dr, La Jolla, CA 92093 (jtully@health.ucsd.edu).

Author Affiliations: Center for Healthcare Cybersecurity, University of California, San Diego, La Jolla (Tully, Straw, Gabriel, Longhurst, Savage, Voelker, Dameff); Department of Anesthesiology, University of California, San Diego, La Jolla (Tully, Gabriel); Department of Computer Science and Engineering, University of California, San Diego, La Jolla (Rao, Savage, Voelker, Dameff); Department of Emergency Medicine, University of California, San Diego, La Jolla (Dameff); Department of Biomedical Informatics, University of California, San Diego Health, San Diego (Gabriel, Longhurst, Dameff).

Author Contributions: Dr Tully and Mr Rao had full access to all of the data in the study and take responsibility for the integrity of the data and the accuracy of the data analysis. Dr Tully and Mr Rao are co-first authors.

Concept and design: All authors.

Acquisition, analysis, or interpretation of data: Tully, Rao, Straw, Savage, Voelker, Dameff.

Drafting of the manuscript: Tully, Rao, Straw, Gabriel, Longhurst, Dameff.

Critical review of the manuscript for important intellectual content: Tully, Straw, Gabriel, Longhurst, Savage, Voelker, Dameff.

Statistical analysis: Tully, Rao, Straw.

Obtained funding: Tully, Dameff.

Administrative, technical, or material support: Straw, Gabriel, Longhurst, Savage, Voelker, Dameff.

Supervision: Tully, Longhurst, Savage, Voelker, Dameff.

Conflict of Interest Disclosures: Drs Tully and Dameff reported serving as cofounders of Inoculum Labs Healthcare outside the submitted work. Drs Tully, Savage, Voelker, and Dameff and Mr Rao have a provisional patent for US 63/674,158 issued to the University of California, San Diego for a digital availability surveillance method, of which they are listed as inventors. No other disclosures were reported.

Funding/Support: This work was supported via contract No. SP4701-23-C-0075 from the Advanced Research Projects Agency for Health (ARPA-H), on which Drs Tully and Dameff serve as co-principal investigators and Drs Gabriel, Longhurst, Savage, and Voelker serve as coinvestigators.

Role of the Funder/Sponsor: ARPA-H had no role in the design and conduct of the study; collection, management, analysis, and interpretation of the data; preparation, review, or approval of the manuscript; and decision to submit the manuscript for publication.

Data Sharing Statement: See Supplement 2.

REFERENCES

1. Menachemi N, Collum TH. Benefits and drawbacks of electronic health record systems. *Risk Manag Healthc Policy*. 2011;4:47-55. doi:10.2147/RMHP.S12985

2. King J, Patel V, Jamoom EW, Furukawa MF. Clinical benefits of electronic health record use: national findings. *Health Serv Res*. 2014;49(1 Pt 2):392-404. doi:10.1111/1475-6773.12135

3. Saiod AK, van Greunen D, Veldsman A. Electronic health records: Benefits and challenges for data quality. In: Khan S, Zomaya A, Abbas A, et al. *Handbook of Large-Scale Distributed Computing in Smart Healthcare*. Springer International Publishing; 2017:123-156. doi:10.1007/978-3-319-58280-1_6

4. Tully J, Selzer J, Phillips JP, O'Connor P, Dameff C. Healthcare challenges in the era of cybersecurity. *Health Secur*. 2020;18(3):228-231. doi:10.1089/hs.2019.0123

5. Dameff C, Tully J, Chan TC, et al. Ransomware attack associated with disruptions at adjacent emergency departments in the US. *JAMA Netw Open*. 2023;6(5):e2312270. doi:10.1001/jamanetworkopen.2023.12270

6. Pham TT, Loo TM, Malhotra A, et al. Ransomware cyberattack associated with cardiac arrest incidence and outcomes at untargeted, adjacent hospitals. *Crit Care Explor*. 2024;6(4):e1079. doi:10.1097/CCE.0000000000001079

7. Neprash HT, Dameff C, Tully J. Cybersecurity lessons from the Change Healthcare attack. *JAMA Intern Med*. 2024;184(11):1283-1284. doi:10.1001/jamainternmed.2024.3162

8. Oliver M, Pearce A, Stillwaugh L, Leszczynski K. The impact of a cyberattack at a radiation oncology department: immediate response and future preparedness. *Adv Radiat Oncol*. 2022;7(5):100896. doi:10.1016/j.adro.2022.100896

9. Sarkissian A. An exploratory analysis of U.S. FDA Class I medical device recalls: 2014-2018. *J Med Eng Technol*. 2018;42(8):595-603. doi:10.1080/03091902.2019.1580778

10. 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;25(2):187-191. doi:10.1093/jamia/ocx057

11. Nelson NC. Downtime procedures for a clinical information system: a critical issue. *J Crit Care*. 2007;22(1):45-50. doi:10.1016/j.jcrc.2007.01.004

12. Dameff C, Pfeffer MA, Longhurst CA. Cybersecurity implications for hospital quality. *Health Serv Res*. 2019;54(5):969-970. doi:10.1111/1475-6773.13202

13. Larsen EP, Rao AH, Sasangohar F. Understanding the scope of downtime threats: a scoping review of downtime-focused literature and news media. *Health Informatics J*. 2020;26(4):2660-2672. doi:10.1177/1460458220918539

14. Wretborn J, Ekelund U, Wilhelms DB. Emergency department workload and crowding during a major electronic health record breakdown. *Front Public Health*. 2019;7:267. doi:10.3389/fpubh.2019.00267

15. Gregory MA. An analysis of the Optus national outage and recommendations for enhanced regulation. *Aust J Telecommun Digit Econ*. 2023;11(4):185-198. doi:10.18080/jtde.v11n4.898

16. Milinic V. Investigating security issues in industrial IoT: a systematic literature review. Updated 2021. Accessed December 12, 2024. https://www.diva-portal.org/smash/record.jsf?pid=diva2:1569644

17. Favarò FM, Jackson DW, Saleh JH, Mavris DN. Software contributions to aircraft adverse events: case studies and analyses of recurrent accident patterns and failure mechanisms. *Reliab Eng Syst Saf*. 2013;113:131-142. doi:10.1016/j.ress.2012.12.018

18. Mugu SR, Zhang B, Kolla H, Balaji SRA, Ranganathan P. Lessons from the CrowdStrike incident: assessing endpoint security vulnerabilities and implications. In: *2024 Cyber Awareness and Research Symposium (CARS)*. IEEE; 2024:1-10. doi:10.1109/CARS61786.2024.10778784

19. Shaji George A. When trust fails: examining systemic risk in the digital economy from the 2024 CrowdStrike outage. *PUMRJ*. 2024;1(2):134-152.

20. Morris JC, Mayer MK. Canaries in coal mines and normal accidents: the CrowdStrike outage and its lessons for critical infrastructure. *J Crit Infrastructure Policy*. Published online September 2, 2024. doi:10.1002/jci3.12021

21. Dunstan J, Easton K, Janda M, et al. Global IT outage: computer havoc caused by CrowdStrike outage could take days to fix- as it happened. *ABC News*. July 19, 2024. Accessed December 12, 2024. https://www.abc.net.au/news/2024-07-19/global-it-outage-CrowdStrike-microsoft-banks-airlines-australia/104119960

22. Cox D. Hospitals around the world are struggling after the great IT meltdown. *Wired*. July 19, 2024. Accessed August 30, 2024. https://www.wired.com/story/hospitals-crowdstrike-microsoft-it-outage-meltdown/

23. Hagland M. Labcorp Systems, Quest Diagnostics, impacted by CrowdStrike-related outage. *Medical Laboratory Observer*. July 26, 2024. Accessed March 27, 2025. https://www.mlo-online.com/online-exclusives/article/55129040/labcorp-systems-quest-diagnostics-impacted-by-crowdstrike-related-outage

24. Dunne J. London Ambulance Service receives 4,500 emergency calls amid global IT outage and 31C heat. *The London Evening Standard*. July 19, 2024. Accessed March 12, 2025. https://www.standard.co.uk/news/london/ambulance-london-it-outage-CrowdStrike-microsoft-nhs-b1171816.html

25. Schulman A, Spring N. Pingin' in the rain. In: *Proceedings of the 2011 ACM SIGCOMM Conference on Internet Measurement Conference*. Association for Computing Machinery; 2011. doi:10.1145/2068816.2068819

26. Padmanabhan R, Schulman A, Dainotti A, Levin D, Spring N. How to find correlated Internet failures. In: Choffnes D, Barcellos M, et al. *Passive and Active Measurement—PAM 2019: Lecture Notes in Computer Science*. Springer; 2019:210-227.

27. Shah A, Fontugne R, Aben E, Pelsser C, Bush R. Disco: fast, good, and cheap outage detection. In: *2017 Network Traffic Measurement and Analysis Conference (TMA)*. IEEE; 2017:1-9. doi:10.23919/TMA.2017.8002902

28. Quan L, Heidemann J, Pradkin Y. Trinocular: understanding Internet reliability through adaptive probing. *Comput Commun Rev*. 2013;43(4):255-266. doi:10.1145/2534169.2486017

29. von Elm E, Altman DG, Egger M, Pocock SJ, Gøtzsche PC, Vandenbroucke JP; STROBE Initiative. The Strengthening the Reporting of Observational Studies in Epidemiology (STROBE) statement: guidelines for reporting observational studies. *Lancet*. 2007;370(9596):1453-1457. doi:10.1016/S0140-6736(07)61602-X

30. Lantern dashboard. Accessed August 5, 2024. https://lantern.healthit.gov/?tab=dashboard_tab

31. Durumeric Z, Wustrow E, Alex Halderman J. ZMap: fast internet-wide scanning and its security applications. In: *Proceedings of the 22nd USENIX Security Symposium*. USENIX; 2013:605-620.

32. Toffalini F, Abbà M, Carra D, Balzarotti D. Google dorks: analysis, creation, and new defenses. In: Caballero J, Zurutuza U, Rodríguez R, et al. *Detection of Intrusions and Malware, and Vulnerability Assessment (DIMVA 2016): Lecture Notes in Computer Science*. Springer; 2016:255-275. doi:10.1007/978-3-319-40667-1_13

33. Jin Y, Tomoishi M, Yamai N. Anomaly detection on user terminals based on outbound traffic filtering by DNS query monitoring and application program identification. In: *Proceedings of the 2021 International Conference on Human-Machine Interaction (ICHMI '21)*. Association for Computing Machinery; 2021.

34. Neprash HT, McGlave CC, Rydberg K, Henning-Smith C. What happens to rural hospitals during a ransomware attack: evidence from Medicare data. *J Rural Health*. 2024;40(4):728-737. doi:10.1111/jrh.12834

35. 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

36. Iacobucci G. Blood donation: NHS stocks are still in short supply after June cyberattack. *BMJ*. 2024;386:q1889. doi:10.1136/bmj.q1889

37. Abouk R, Powell D. Ransomware attacks, ED visits and inpatient admissions in targeted and nearby hospitals. *JAMA*. 2024;331(24):2129-2131. doi:10.1001/jama.2024.7752

38. Scantlebury A, Sheard L, Fedell C, Wright J. What are the implications for patient safety and experience of a major healthcare IT breakdown: a qualitative study. *Digit Health*. Published online April 19, 2021. doi:10.1177/20552076211010033

39. Kim MO, Coiera E, Magrabi F. Problems with health information technology and their effects on care delivery and patient outcomes: a systematic review. *J Am Med Inform Assoc*. 2017;24(2):246-250. doi:10.1093/jamia/ocw154

40. van Boven LS, Kusters RWJ, Klokman VW, Dameff C, Barten DG. Acute care disruptions due to information technology failures in the Netherlands from 2000 to 2020. *Health Policy Technol*. 2024;13(2):100840. doi:10.1016/j.hlpt.2024.100840

41. Kanter GP, Rekowski JR, Kannarkat JT. Lessons from the Change Healthcare ransomware attack. *JAMA Health Forum*. 2024;5(9):e242764. doi:10.1001/jamahealthforum.2024.2764

42. Groseclose SL, Buckeridge DL. Public health surveillance systems: Recent advances in their use and evaluation. *Annu Rev Public Health*. 2017;38:57-79. doi:10.1146/annurev-publhealth-031816-044348

43. Choi J, Cho Y, Shim E, Woo H. Web-based infectious disease surveillance systems and public health perspectives: a systematic review. *BMC Public Health*. 2016;16(1):1238. doi:10.1186/s12889-016-3893-0

44. Milinovich GJ, Williams GM, Clements ACA, Hu W. Internet-based surveillance systems for monitoring emerging infectious diseases. *Lancet Infect Dis*. 2014;14(2):160-168. doi:10.1016/S1473-3099(13)70244-5

45. Gummin DD, Mowry JB, Beuhler MC, et al. 2022 Annual report of the National Poison Data System (NPDS) from America's Poison Centers: 40th annual report. *Clin Toxicol (Phila)*. 2023;61(10):717-939. doi:10.1080/15563650.2023.2268981

46. Diguisto C, Saucedo M, Kallianidis A, et al. Maternal mortality in eight European countries with enhanced surveillance systems: descriptive population based study. *BMJ*. 2022;379:e070621. doi:10.1136/bmj-2022-070621

47. Zeng D, Cao Z, Neill DB. Artificial intelligence–enabled public health surveillance—from local detection to global epidemic monitoring and control. In: Xing L, Giger ML, Min JK, et al. *Artificial Intelligence in Medicine*. Academic Press; 2021:437-453. doi:10.1016/B978-0-12-821259-2.00022-3

48. Balsari S, Kiang MV, Buckee CO. Data in crisis—rethinking disaster preparedness in the United States. *N Engl J Med*. 2021;385(16):1526-1530. doi:10.1056/NEJMms2104654

49. Jayawardene V, Huggins TJ, Prasanna R, Fakhruddin B. The role of data and information quality during disaster response decision-making. *Prog Disaster Sci*. 2021;12:100202. doi:10.1016/j.pdisas.2021.100202

50. Fakhruddin B, Kirsch-Wood J, Niyogi D, Guoqing L, Murray V, Frolova N. Harnessing risk-informed data for disaster and climate resilience. *Prog Disaster Sci*. 2022;16:100254. doi:10.1016/j.pdisas.2022.100254

51. Kubo T, Yanasan A, Herbosa T, Buddh N, Fernando F, Kayano R. Health data collection before, during and after emergencies and disasters—the result of the Kobe expert meeting. *Int J Environ Res Public Health*. 2019;16(5):893. doi:10.3390/ijerph16050893

SUPPLEMENT 1.

eTable. Example Table of Services Affected by CrowdStrike Outage and the Techniques Used to Translate the Services to Their Clinical Context

SUPPLEMENT 2.

Data Sharing Statement