News and Perspectives

What Health Care Organizations Have Learned From Telecommunication Outages

Catharine Solomon, JMIR Correspondent

Key Takeaways

- Health care facilities' ability to provide patient care can be threatened by large-scale telecommunication outages, requiring providers to build additional redundancy into their own infrastructure.
- While steps have been taken to formalize accountability for some telecommunication providers (such as, in Canada, via the Memorandum of Understanding on Telecommunications Reliability), gaps remain.

Telecommunication (telecom) breakdowns at massive scales are fresh in recent memory; in Canada, the Rogers Communications outage of July 2022 cut off over 12 million users' wireless and wire-line services for over 24 hours [1], and in 2024, a single faulty update to CrowdStrike's cybersecurity software caused an estimated 8.5 million Microsoft systems worldwide to crash [2]. In the past several months alone, widespread outages from internet infrastructure providers, like Cloudflare and Amazon Web Services (AWS), have alerted users to the fragility of an internet that relies on a handful of companies to function [3].

Health care facilities, which use telecom for everything from faxing prescriptions, to accessing electronic health records (EHRs), to virtual care, have to navigate these breakdowns under an additional unique pressure: their patients' well-being on the line. In the months and years following major outages, health care institutions have taken steps to mitigate the threat of service disruption to patient care.

The Rogers Outage

On the morning of July 8, 2022, Canadians woke up to a phone and internet outage hitting nearly every sector. While upgrading their IP core network, Rogers staff had removed a policy filter, which allowed IP routing data to flood and then crash the core routers, leaving user traffic unable to reach their destinations and over 12 million Rogers users without service [1].

Many of these users were health care providers and organizations, as well as patients trying to access health care. Family medicine clinics found themselves suddenly unable to carry out basic functions, like faxing prescriptions, scheduling appointments, and attending virtual care appointments [4]. The outage disproportionately affected health care services in remote locations, which often rely on network access to consult with specialists; this was compounded by the loss of connectivity across other health system partners [4]. In Toronto, immunization clinics lost access to the provincial COVID-19 vaccination management system, long-term care facilities lost access to their residents' EHRs [5], and hospitals had to scramble to mitigate the outage's effects on patient care.

According to Michael Garron Hospital's (MGH's) Chief Information Officer Amelia Hoyt, the brunt of the outage at MGH fell on corporate staff, who use Rogers cellular services for their work phones. This loss of corporate cellular mobility threatened patient care only indirectly, but physicians who relied on Rogers for their own mobile phones also couldn't be reached. MGH leadership gathered an emergency command center to develop a plan for how to navigate the outage.

"We did need to come together to figure out how to make sure that we didn't have delayed communications that inadvertently would affect patient care," says Hoyt. The solution in the moment was to identify affected staff and, by using a fan-out list, set alternate communication routes.

The outage allowed Hoyt and her team to identify a gap in their IT strategy and then fix it. "We had no other redundancy for if cell services are down." Redundancy—the strategy of duplicating system components or functions—works by keeping fail-safes and backup components at the ready.

"What we decided to do was invest in eSIMs from a different cellular provider for corporate mobile devices," she explains, "loaded onto select individuals' phones....If Rogers went down again, we would be able to activate this alternate provider's eSIM, and that would allow for continuity."

The CrowdStrike Outage

On July 19, 2024, University Health Network (UHN) staff trying to connect with clinical systems were met instead with blue error screens. A defective content configuration update released by the cybersecurity company CrowdStrike had caused millions of Windows hosts worldwide to crash, resulting in disruption of services across multiple industries and organizations, including government agencies, airlines, health care facilities, and even 911 connectivity in some areas [6,7]. In the health care sector, the outage disrupted everything from EHR access, to telemonitoring, to operational management, to research [8].

According to Carl Virtanen—chief technology officer for UHN Digital (UHN's IT department)—the UHN's downtime procedures for switching to manual documentation helped mitigate disruptions to patient care, though several nonurgent appointments had to be rescheduled.

"UHN was able to prevent more significant technological disruption by pausing software updates and limiting the number of devices affected by the CrowdStrike outage," Virtanen says, noting that UHN Digital's protocols, which include prioritizing critical areas (such as emergency departments, intensive care units, and operating rooms) when responding to technological problems, have not been updated since. "All critical clinical systems were back up and running normally by the end of the day the outage began."

Importance of Redundancy

The telecom ecosystem is deeply interconnected. For complex critical systems, like health care, that rely on telecoms [9], interconnectivity facilitates seamless and efficient data sharing across a network of health system partners. But these interconnected systems can be disrupted on a large scale by a single point of failure in the infrastructure upon which they depend. So, how can disruptions be avoided?

Virtanen says that the best strategy for avoiding downtime is already, ideally, in use: "It is critical to have redundancy layers built into technical infrastructure to maintain operational efficacy in the event of service disruptions, such as the CrowdStrike outage."

On the most basic level—the physical infrastructure underpinning telecom services—a lack of redundancy can result in, for example, a beaver taking out nearly half of a town's internet connection by chewing through the network's single fiber-optic cable [10]. The 2022 Rogers outage itself exemplified the peril of putting all of one's technological eggs in one basket; since the Rogers management network relied on the very IP core network that had crashed, staff struggled to communicate with one another and remotely investigate the issue, delaying repairs for hours [1].

Health care facilities' preparations for outages, such as MGH's eSIM investment and UHN's downtime protocol of switching to paper records, act as another redundancy layer. In a perfect world with an unlimited budget, Hoyt says that her team would invest in additional redundancy for all IT services at MGH; at one point, they had even toyed with the idea of low-tech backups, like walkie-talkies. The solution is practical but not without its drawbacks; maintaining redundant systems can be cost-intensive, particularly for health care facilities with fewer resources [4].

Who's Accountable?

The fallout and appropriate redress of telecom outages have often been framed in terms of monetary loss, which can be reimbursed through vendor refunds and credits [5]. But when essential services, like health care, rely on network access to function efficiently and effectively, a framework that accounts only for economic impact falls short.

"Telecommunication is really foundational," says Hoyt. "I liken it to 911 service—there are some standards that are expected, that you should be able to require some of these telecom companies to follow."

Steps have been taken to hold Canadian telecom companies accountable for the essential services they provide; in September 2022, thirteen major telecom companies signed the Memorandum of Understanding (MOU) on Telecommunications Reliability [11]. The signatories of this MOU agreed to provide one another with emergency roaming and assistance in the event of a major outage, building ready-to-go redundancy into Canadian telecom services.

The MOU is "a positive step," according to Hoyt. "What will be interesting to see is how this agreement is put into practice if and when the next unplanned outage occurs."

What about the rest of the telecom ecosystem? Health care organizations' ability to access and relay information is only as stable as the infrastructure they use to communicate, and unlike health care providers who can be held liable for medical malpractice or medical devices that are held to rigorous standards of reliability and accuracy, many telecom services—particularly newer cloud-based models, like software as a service, that boast cost-effective scalability for clients—have frequent downtimes without consequence.

For health care organizations, using third-party services carries an inherent risk: tech disruptions that can't be addressed in-house. "When the infrastructure is under local IT's control, like my department, it's something my team would have more direct accountability for," says Hoyt. "If AWS is out, then you're kind of stuck between a rock and a hard place. There's nothing really a local IT team can do about that because we actually don't have any control over it."

Health care organizations must weigh this risk in choosing whether and when to rely on such services. Unless these services are reliable enough to meet health care standards, the scalability boost may not be worth it.

As more and more of our essential systems rely upon telecom infrastructure, redundancy and resiliency strategies are key to avoiding more outages that, at best, create delays and administrative burden in health care and, at worst, can lead to real patient harm. In an interconnected telecom ecosystem, all providers, companies, and organizations have the opportunity and the responsibility to do their part in keeping critical services running smoothly.

Keywords: telecommunications; telecommunications standards; health services administration; health care quality; access; evaluation; infrastructure; risk management; emergency preparedness; health care resiliency

Conflicts of Interest

None declared.

References

1. Xona Partners Inc. Assessment of Rogers networks for resiliency and reliability following the 8 July 2022 outage – executive summary. Canadian Radio-television and Telecommunications Commission. Jul 2024. URL: https://crtc.gc.ca/eng/publications/reports/xona2024.htm [Accessed 2026-01-27]
2. Weston D. Helping our customers through the CrowdStrike outage. Official Microsoft Blog. Jul 20, 2024. URL: https://blogs.microsoft.com/blog/2024/07/20/helping-our-customers-through-the-crowdstrike-outage/ [Accessed 2026-01-27]
3. London tech expert explains why the internet blew up this week (temporarily). CBC News. Nov 22, 2025. URL: https://www.cbc.ca/news/canada/london/london-tech-expert-explains-why-the-internet-blew-up-this-week-temporarily-9.6987955 [Accessed 2026-01-27]
4. Li T, Tran C, Yung A, Thomas A. Family physicians and the nationwide communications service outage in Canada. Canadian Family Physician. Dec 9, 2022. URL: https://www.cfp.ca/news/2022/12/09/12-09 [Accessed 2026-01-27]
5. Attachment 3: Rogers Communications July 2022 outage impact: economic, operational & potential for ConnectTO to mitigate future events. City of Toronto. URL: https://www.toronto.ca/legdocs/mmis/2023/ex/bgrd/backgroundfile-239381.pdf [Accessed 2026-01-27]
6. Gallagher JC, Pechtol CL. CrowdStrike IT outage: impacts to public safety systems and considerations for Congress. Congress.gov. Dec 4, 2024. URL: https://www.congress.gov/crs-product/IF12717 [Accessed 2026-01-27]
7. Ellingson C. Global software glitch affected Edmonton police 9-1-1 calls overnight Friday. CTV News. Jul 19, 2024. URL: https://www.ctvnews.ca/edmonton/article/global-software-glitch-affected-edmonton-police-9-1-1-calls-overnight-friday/ [Accessed 2026-01-27]
8. Tully JL, Rao S, Straw I, et al. Patient care technology disruptions associated with the CrowdStrike outage. JAMA Netw Open. Jul 1, 2025;8(7):e2530226. [doi: 10.1001/jamanetworkopen.2025.30226] [Medline: 40682764]
9. Howell B. Beyond infrastructure: internet ecosystem resilience and the public good. Telecomm Policy. Aug 2025;49(7):102998. [doi: 10.1016/j.telpol.2025.102998]
10. Hundreds lose internet service in northern B.C. after beaver chews through cable. CBC News. Apr 25, 2021. URL: https://www.cbc.ca/news/canada/british-columbia/beaver-internet-down-tumbler-ridge-1.6001594 [Accessed 2026-01-27]
11. Memorandum of Understanding on Telecommunications Reliability. Innovation, Science and Economic Development Canada. URL: https://ised-isde.canada.ca/site/ised/en/memorandum-understanding-telecommunications-reliability [Accessed 2026-01-27]

Please cite as:
Solomon C
What Health Care Organizations Have Learned From Telecommunication Outages
J Med Internet Res 2026;28:e91456
URL: https://www.jmir.org/2026/1/e91456
doi: 10.2196/91456