



Building resilient systems to protect continuity of patient care

Public healthcare provider | Healthcare



Business opportunity

Over a million people annually depend on a U.S. public healthcare provider for regular check-ups, urgent care and specialized treatments such as organ transplants.

Across its state-of-the-art facilities, the organization uses a myriad of digital systems to run health screenings, dispense medication, and manage complex programs of care. Although the organization's growing digitalization had increased operational efficiency and improved patient care, the complexity of its IT environment also increased the risk of cyber threats that could result in unplanned downtime.

The healthcare provider had a well-functioning Security Information and Event Management (SIEM) solution. However, they knew that sophisticated bad actors could take even well-defended production systems offline for weeks.

With lives on the line and strict regulations to uphold, the healthcare provider's end goal was a continuously-operated minimum viable hospital, with the capability to handle disruptions in minutes.

Technical challenge

The healthcare provider operated from a primary data center, backing up data to a secondary site without the redundant systems needed to continue operations in case of a catastrophic outage. That hot-cold disaster recovery model supported a Recovery Time Objective (RTO) of 31 days.

The healthcare provider was experiencing data growth rates of 30% year-on-year. Their existing data protection solution was sometimes unable to complete backups within scheduled windows. Even with full backups, should a bad actor infiltrate the production environment, the healthcare provider did not know if and when their backups were also compromised. That vulnerability could complicate recovery from lesser disruptions and jeopardize recovery from a catastrophic outage.

Since the healthcare provider was already in the process of transitioning to a cloud-based electronic health record (EHR) system, modernizing their disaster recovery solution required cloud-readiness.

Our solution

Together, as an important step towards increased availability, the healthcare provider and Kyndryl co-created a future-ready disaster recovery solution that uses AI to proactively scan for threats in backups, and uses a single dashboard for both monitoring and recovery.

Kyndryl first reassessed the provider's overall recoverability thresholds in the event of a major outage, evaluating best-fit options for an IT estate that was on premises but would migrate onto a cloud platform. The healthcare provider chose the Kyndryl Rubrik Cyber Incident Recovery solution to cost-effectively and flexibly meet its current and future requirements.

Kyndryl experts and the healthcare provider's IT team then partnered to migrate nearly 1,800 systems to Rubrik Enterprise on Microsoft Azure, where mission-critical EHR workloads would run. Rubrik's immutable, cloud-archived and air-gapped data backup vaults support data integrity and recoverability, even in cases of total disaster at the production site.

The solution enables the healthcare provider to orchestrate the tasks that automatically recover the core systems needed to run a minimum viable hospital even before a full recovery finishes.

Through Rubrik's AI capabilities, the solution also discovers unprotected data across the healthcare provider's application estate and actively identifies anomalies in backed-up data. The solution has already alerted the healthcare provider's Security Information and Event Management (SIEM) of two real threats in the early weeks of operation.

The power of partnership

The combined expertise of the Kyndryl and Rubrik teams in managing cybersecurity operations for large enterprises helped the healthcare provider cut time-to-value for its new solution.

Kyndryl's strategic partnership with Microsoft helped the team design a robust Azure infrastructure that will support growing data volumes.

What progress looks like

Through this transformation, the healthcare provider proactively improved its cybersecurity posture with automated recovery processes configured to restore a minimum viable hospital in the event of downtime.

Other results so far:

- 50% reduction in recovery time objective (RTO) from 31 to 15 days gets hospital systems up and running faster to support patient care after a catastrophic outage
- 75% faster EHR database backup – from 50 hours to 7 hours increases the readiness for recovery in the event of an outage
- 99% reduction in build-to-hand-off times for new server systems enables the IT team to quickly expand backup capacity as data grows
- 20% reduction in backup costs

Meet the team

Greg Craighead
Client Partner, Kyndryl



Sujay Ghosal
Delivery Partner, Kyndryl



Jeff Dean
Chief Enterprise Architect, Kyndryl



Ray Ondrick
Director, Technical Solutioning, Kyndryl



Robert Mathews
Lead Project Manager, Kyndryl



Angie Wells
Deal Maker, Kyndryl



Manish Lall
Program Manager, Kyndryl



What's your next digital business challenge? Let's tackle it together.

[Talk to an expert](#) →

kyndryl.

© Copyright Kyndryl, Inc. March 2026

Kyndryl is a trademark or registered trademark of Kyndryl Inc. in the United States and/or other countries. Other product and service names may be trademarks of Kyndryl Inc. or other companies. This document is current as of the initial date of publication and may be changed by Kyndryl at any time without notice.