Business Continuity | Cybersecurity | Healthcare Information Systems | IT Challenges

3 Unsolved business continuity problems for hospitals

By Steve McDonald | May 23, 2022

As U.S. hospitals continue to face slim operating margins, staffing shortages, and mergers and acquisitions, they're more focused than they've ever been on delivering optimal care, prioritizing patient safety, and mitigating risk to stay afloat. At the same time, they're facing an increasing amount of business continuity problems that could pose a threat to their operations and their patients' lives.

For starters, multi-disciplinary teams are sharing a vast amount of information but their communications systems are often fragmented and ineffective.

According to a 2020 report by ECRI, as a result of multiple provider settings for care delivery, care fragmentation is among the top 10 patient safety concerns because it disrupts communication between providers and affects care coordination.

Plus, while the reliance on information technology has helped drive operational efficiency, a downtime event or cyber-attack can seriously impact patient safety and hospital operations. In fact, cyber-attacks against healthcare organizations increased 45% since November 2021, a recent report found.

Unsolved business continuity problems for hospitals

CIOs, CTOs, and IT staff are continually looking for ways to ensure care continuity during downtimes and seamless communications, prevent the loss of critical information, and manage inevitable downtime events.

Here are 3 unsolved business continuity problems today's hospitals are facing—and how to best address them.

1. Complicated hospital communications

Multi-disciplinary teams need information that goes above and beyond the EHR, yet with so many additional, disparate sources, including telehealth, mobile health apps, RPM, and wearables, as well as various formats and destinations, gaps can occur that can lead to patient safety issues.

Fragmented, complicated hospital communication workflows also contribute to the frustration that overwhelmed staff are already feeling, which can also reduce referrals and negatively affect the care patients receive.

2. Managing downtime events and cyberattacks

Planned downtimes such as a server migration or software update, and unplanned downtime events such as fires, power outages, natural disasters, and cyber-attacks are all significant business continuity problems for today's hospitals.

When downtimes occur, clinical care teams often revert to manual, paper processes, lack clinical decision support during documentation, and have to piece together information to understand a patient's entire journey across the episode of care.

While hospitals may rely on frequent back-ups, they may not always have access to the right information.

What's more, if a cyberattack occurs, back-ups could duplicate the malware, creating an even bigger problem and require additional work to make sure the systems are free and clear of viruses.

According to a 2019 report by Netwrix, 32% of healthcare organizations store critical data in the cloud, yet 18% say they would consider moving their data back on-premises, citing security concerns (56%), reliability and performance issues (22%), and high costs (22%) the cloud carries.

To ensure clinical and business continuity, hospitals need access to critical patient data when they're online or offline. Secure patient data accessibility during downtimes also ensures that providers have read lab results, reports, and other important information throughout a patient's care journey to ensure proper care continuity.

3. Interoperability

Interoperability continues to be one of the most significant business continuity problems for hospitals, particularly because of the vast amount of data and the need for interconnected systems across healthcare systems and facilities.

Additionally, the COVID-19 pandemic has brought to light the importance of exchanging data accurately, securely, easily, and in a timely, automated manner.

Still, research shows many hospitals have made progress. According to the 2019 American Hospital Association IT Supplement published by the Office of the National Coordinator (ONC) for Health IT, 55% of acute care hospitals participated in all four interoperability domains (send, receive, find, and integrate), up from 26% in 2015.

Although HL7 was meant to standardize the exchange of information, it's not a plug-and-play solution. Variations exist so hospitals still need to make sure that the right information is sent, in the right format, and is in the right place.

How hospitals can solve for business continuity challenges

Our new Beacon platform enables secure access to—and availability of—critical hospital information during planned, unplanned, or cyber-attack events to ensure clinical and business continuity and patient safety.

Our vendor-agnostic solution offers process automation and workflow capabilities that allow hospitals to manage and deliver messages encrypted in a HIPAA-compliant format, and tailored according to individual user preferences within and outside a health system.

To learn more or schedule a demo, contact us today.