Business Continuity | IT Challenges

Is your hospital unwittingly making these healthcare downtime mistakes?

By Steve McDonald | June 6, 2022

Whether it's planned, unplanned, or cyberattack events, healthcare downtimes at hospitals in the U.S. are inevitable.

A downtime can include something as small as the EHR being unavailable at a particular workstation to something more widespread like a network and internet outage that affects all workstations throughout a health system.

Regardless of how significant the downtime is, however, the impact can be felt throughout a health system and its patients.

Cyberattacks, in particular, are on the rise and now a top priority for hospitals.

A recent Bloomberg survey of CTOs from various industries, including healthcare, found that cybersecurity was an area of expertise demanded most at their organizations, and 61% will increase technology spending in the next 12 months.

Unfortunately, most hospitals we speak to don't have a technology-driven downtime strategy in place, often because they think that identifying a solution is too time-consuming or arduous to deploy.

Or they have an outdated or limited mitigation strategy which isn't enough.

While some hospitals do have a solution in place, it's often costly and may not be reliable enough to ensure care continuity during downtimes.

What's more, when the internet or network is down, oftentimes the cloud-based solutions are not equipped to provide on-premise information at the point of care because their solutions rely on the cloud.

Techno-iatrogenesis has created this inability to function when the EMR is not available.

When the EMR or network is unavailable, clinicians react like teenagers who had their smartphones taken away.

5 Healthcare downtime mistakes to avoid

Although hospitals know how costly downtime events can be, most make crucial mistakes when it comes to having a strategy in place.

1. Paper processes

Most hospitals have an unnecessary dependency on paper during downtimes—printing copies of records and distributing them to staff.

Not only is this time-consuming and costly—and can lead to frustration, stress, and burnout—but the patient's care journey becomes fragmented, and safety risks can surface.

Without all of the critical information about a patient's care journey and clinical decision support that's available in the EHR, providers are forced to piece everything together and try to paint the whole picture.

Relying on paper records also runs the risk that they will get mixed up or misplaced.

And if providers don't get the information they need in a timely manner, errors can occur.

2. False reliance on the cloud

Many hospitals think that when it comes to their healthcare downtime strategy, the cloud is the optimal solution, but research shows it may not be.

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.

The reasons?

- Security concerns (56%)
- Reliability and performance issues (22%)
- High costs (22%) associated with the cloud

While the cloud can be a backup, it's not protection from monthly security patches, migrations, upgrades, and inevitable downtimes such as downed wires, brownouts, and cyberattacks, nor does it provide access to critical information.

3. Lack of team mentality

A common mistake hospitals make is failing to take a team approach.

Yet a healthcare downtime strategy is an all-hands-on-deck initiative that includes a downtime planning committee comprised of emergency response, clinical informatics, IT, operations, business continuity, clinical areas, and other departments that are a part of all the downtime procedures.

Additionally, hospitals may consider a tiered downtime response system such as the one at Massachusetts General Hospital Center for Disaster Medicine, which is flexible and can be adjusted to each downtime event.

4. Thinking a disaster recovery plan is a downtime strategy

While hospitals need a disaster recovery plan, thinking it's the downtime solution is a myth.

With disaster recovery, there's a time lag, and it could be 36 hours or more before the EHR is back online.

Some hospitals rely on frequent back-ups alone, but that doesn't always ensure they will have access to critical patient information.

Not to mention that if there's a cyberattack, back-ups can duplicate malware, which can spread throughout the network and trigger down the line, creating an even bigger problem.

Having an isolated, on-site, and cloud-based server, therefore, is important.

5. Failing to update the downtime strategy

Oftentimes, hospitals develop a downtime strategy procedure to satisfy a HIPAA-compliant mandate but never give it a second look.

It's important, therefore, to conduct health checks on a quarterly basis to make sure what was developed is still relevant.

What to look for in a healthcare downtime solution

For hospitals looking for a healthcare downtime solution, it's important to identify one that has certain features, including:

- Simple to deploy and available the moment systems go down to ensure care continuity.
- Access to critical information in all areas where care is administered and the ability to deliver encrypted reports at the point of care.
- Isolated, on-premise, or cloud-based secure server that is outside of the network.
- Capability to process new patients with barcodes and capture documentation and charges during downtimes.
- Flexibility and the ability to personalize the types of data that need to be accessed.
- An air gap server that is protected from cyberattacks.

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