Business Continuity | Cybersecurity | IT Challenges

6 Factors to consider when calculating real EHR downtime costs

By Steve McDonald | June 20, 2022

Hospitals in the U.S. rely heavily on their electronic health record (EHR) every day to deliver safe care, ensure care continuity, improve health outcomes, and drive operational efficiency, including optimizing the revenue cycle.

Yet when the systems go down, understanding the true reality of EHR downtime costs—and all the nuances associated with an event—can be eye-opening.

Between 2012 and 2018, 166 hospitals had 701 days of downtime in 43 events, and nearly half of the events were cyberattacks, a 2020 study in the Health Informatics Journal found.

Both planned and unplanned downtime and cyber events cause a significant and immediate impact on operations and care, leave a hospital vulnerable to patient safety and compliance risks, cause a ripple effect across all departments, and lead to negative downstream effects that drive costs and impact long-term profitability.

The true picture of EHR downtime costs

As hospitals continue to cope with slim operating margins, high costs, and labor shortages, it's imperative that they look at how to calculate EHR downtime costs to understand the full impact on their bottom line.

Here's what your hospital should keep in mind when you're calculating EHR downtime costs.

1. Operations that are modified—or have come to a halt

One of the most significant EHR downtime costs are attributed to hospital operations that must be altered or stopped altogether.

Without the EHR, care continuity during downtime can be significantly impacted.

Doctors don't have access to their patients' medical history, medications, and other critical data, they lack clinical decision support during documentation, and may have to revert to manual, paper processes that waste time, resources, and money.

An EHR downtime may also prevent hospitals from admitting new patients, performing procedures and surgery, and sending prescriptions, to name a few.

A 2019 study in the journal Applied Clinical Informatics, conducted at two U.S. hospitals, found that during a downtime, lab test results were delayed by an average of 62% compared to normal operations.

Hospitals also may not be able to provide the appropriate level of care and have to transfer patients in the ICU to other hospitals, for example.

Revenue cycle disruptions and lost charges are equally problematic, and a major concern when a cyberattack event lasts more than a few weeks.

The real financial cost to hospitals is astronomical, and it has deep downstream effects on cash flow and operations.

2. Patient safety risks

A lack of clinical data access during downtimes and cyber events can lead to a lack of care coordination, treatment delays, medical errors, and other risks to patient safety.

For example, medications—and the dose—can be incorrectly prescribed or administered, leading to adverse drug reactions, allergic reactions, and the potential for hospital readmissions.

Plus, downtime and cyber events can prevent hospitals from having critical, life-saving information when unresponsive patients arrive in the ED.

3. Recovery efforts and audits

Cyberattacks in healthcare are on the rise, with nearly 50% of hospital executives who say they had to shut down because of a cyberattack in the last 6 months, a 2021 report found.

Of those:

- Large hospitals were down for 6.2 hours on average, costing them $21,500 per hour.
- Midsize hospitals were down for 10 hours on average, costing them $45,700 per hour.

When an EHR downtime event occurs due to a cyberattack, the IT team will be focused on bringing systems back online, recovering patient records, conducting system audits, and protecting patient privacy—all of which contribute to costs.

4. Staff productivity

Another factor to consider when it comes to calculating EHR downtime costs are altered workflows and reduced staff productivity.

Staff are not able to do their jobs as well, or the hospital may have to pay staff who are unable to work.

Plus, the frustration, stress, and burnout they experience because of an EHR downtime can all drive costs.

5. Reputation and referrals

It's also important to look at the long-term effects and damage downtime and cyber events can have on a hospital's reputation.

Without access to treatment and medication updates, patient satisfaction,

HCAHPS scores, patient loyalty, and word-of-mouth referrals can all be negatively impacted, which can affect a hospital's long-term profitability.

Additionally, there are likely costs associated with marketing and public relations efforts to restore trust in the organization and rebuild their reputation and brand recognition.

6. Compliance violations

Data breaches that result from EHR downtimes are costly for hospitals.

According to Ponemon Institute's annual Cost of a Data Breach Report, for the tenth consecutive year, healthcare had the highest average breach costs which totaled $7.13 million—up 10.5% since 2019.

Losing data in and of itself is costly, but downtime and cyber events that compromise protected health information (PHI) can also be a compliance risk.

The HIPAA Privacy Rule mandates hospitals to comply with its data security and integrity standards, and the penalties and fines for noncompliance are substantial—up to $50,000 per violation.

Now is the time for hospitals to look to new solutions to protect their patients and their organizations during downtime events and drive revenue.

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.

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