INTERBIT DATA *Software to Improve Healthcare Efficiency*

WHITEPAPER

Healthcare Business Continuance: Implementing Procedures to Address Critical System Downtimes

Introduction

Network, system and power outages occur annually, and always at a cost to the organization in terms of interrupted workflow and impacted patient service, not to mention the hit it takes at the bottom line. Your healthcare information system (HCIS), which houses all your patient information, can be brought down for reasons that are planned (maintenance, upgrades, etc.), but unplanned downtimes can occur due to a number of reasons, including a loss of power, network connectivity, natural disaster, or even a system failure.

Any downtime of your HCIS means that your clinicians will be unable to access critical patient data, including any updated medication records, which will interrupt the delivery of patient care and impact patient safety.

Given that patient care and safety are something you don't want to risk, does your organization have a set of procedures in place in the event a system downtime occurs?

The Situation: Inevitable Healthcare Information System Downtime

What goes up must come down. As healthcare processes have become more and more automated and healthcare organizations transferred to electronic health records to simplify patient data management, a new set of challenges has emerged. Security of electronic patient data is one, mainly due to HIPAA and other governmental regulations.

System reliability is another challenge. As much as technology has improved, it still suffers from both planned and unplanned downtimes. In fact, downtimes of various types occur more often than your organization may realize. Software, hardware, and network upgrades and updates still affect the overall uptime of your systems and users.

Many downtimes are not even reported or recorded because they have occurred for what is considered to be a short period of time. Based on a healthcare organization's downtime policies and procedures, a system could be down for minutes or even hours before or without an official downtime being declared. Meanwhile, the undocumented downtime's impact could be significant, as processes will still experience diminished efficiency during that timeframe.

251 West Central St., Ste. 36, Natick MA 01760
508.647.0013 | www.interbitdata.com

FREQUENCY OF DOWNTIMES

The frequency and duration of unplanned downtimes pose a challenge for healthcare facilities — problems made worse as the cost of downtimes soars over time.

A December 2013 survey sponsored by Emerson Network Power and conducted by the Ponemon Institute revealed that healthcare facilities average 2.7 *complete* healthcare information system outages over a two-year period, the most compared with other markets surveyed, including communications, financial services, retail, education, public sector, hospitality and several others. In addition, healthcare facilities have the second longest average downtimes at 122 minutes per incident.

The healthcare facilities surveyed also experienced an average of six partial outages during the same two-year timeframe. The average number of device-level outages, or those limited to individual servers, was the highest at 11 outages in two years.

THE COST OF DOWNTIMES

Healthcare organizations face average costs of $690,000 per downtime incident, according to the findings of the Ponemon Institute study. This is roughly a 41 percent increase over what was reported in 2010. Of course, those numbers depend on several factors, which include the length of the downtime and its complexity, but overall, organizations typically have to shell out over $7,900 per minute of downtime.

“This increase in cost underscores the importance for organizations to make it a priority to minimize the risk of downtime that can potentially cost thousands of dollars per minute,” said Ponemon in the report.

The most significant cost organizations incurred after data center or system outages were business disruption costs, pegged at an average of $238,717; lost revenue costs, averaging $183,724; and end-user productivity, an average of $140,543 lost per incident, according to the report. Out of 15 industry sectors covered in the report, healthcare saw the 7th highest costs, above retail, transportation, technology and software, co-location, services, media, education, public sector and hospitality sectors.

REAL IMPACT OF DOWNTIMES IN HEALTHCARE

When a system downtime occurs in a healthcare facility, the financial costs incurred are really the least of the organization’s concerns. There are serious potential consequences involving patient safety and the delivery of patient care.

When your healthcare information system goes down, your clinicians are not only unable to access the patient information they need — they’re unable to access the most up-to-date information. Changes in patients’ medications and treatments often occur and nurses and other clinicians need to be informed of any new status with a patient. If, for instance, they are not aware that a patient has developed an allergic reaction to a previously-prescribed medication and then administers that med based on an older medication record, the results could be disastrous.

The disruption to patient-specific processes and workflow when a system downtime occurs leads to diminished responsiveness to patients and interruptions in the delivery of patient care. Essentially, your clinicians’ ability to provide quality care is compromised. If they are unable to access the information they need from the healthcare information system to do their jobs and treat their patient, patients will suffer the consequences. Patient satisfaction is critical to your business, as it impacts your HCAHPS scores and the public perceptions and investments that are tied to them. However, a patient fatality that results from slow responsiveness or the use of out-of-date information can cost your organization far more than its reputation and customer service scores.

HIPAA REQUIREMENTS FOR PATIENT DATA SECURITY AND BUSINESS CONTINUITY

HIPAA’s “Security Guidelines” mandate that all healthcare organizations using healthcare data comply with its data security and business continuity standards, and the penalties and fines for noncompliance are substantial. A contingency plan for disaster recovery and business continuity is a key standard stipulated in the HIPAA Security Rules under the Administrative Safeguards Section.

The contingency plan should address data availability and the risks a business disruption poses to that availability. The goal

is to ensure that staff can still access vital systems and data in spite of the disruption. The contingency plan should also outline strategies for implementing various technical measures, procedures and plans to ensure the recovery of networking systems, data and operations in the event of a disruption and to ensure the hospital is able to resume to its normal functions in the event of a crisis, disaster or disruption.

Why Hospitals Need to Ensure Downtime Business Continuance

CASE STUDY: SUTTER HEALTH SYSTEM

In August 2013, the 24-hospital Sutter Health System in Northern California reported that a software glitch with its $1 billion electronic health record system made it inaccessible to clinical staff. According to reports, the system outages across the hospitals lasted a full day.

"Many of the families became concerned because they noticed the patients were not getting their medications throughout the day," explained Mike Hill, an RN at Sutter's Alta Bates Summit Medical Center and a California Nurses Association representative for the hospital. "Meds were not given for the entire day for many of the patients."

CASE STUDY: FIONA STANLEY HOSPITAL

In February 2015, doctors, nurses and administrators at Fiona Stanley Hospital, Australia's most technologically-advanced hospital had to revert to "downtime procedures" when WA Health's computer systems crashed for more than 14 hours during an outage caused by lightning storms.

According to the local health department, the crash resulted in the loss of clinical and non-clinical computer applications and the IT network, including email, forcing the staff to use pens and paper and then enter patient data once the system came back online.

While the hospital had downtime procedures and business continuity plans in place to ensure patient safety was never compromised, the staff still had to resort to manual processes, and later, take the time to enter patient updates to the system, significantly reducing their productivity and responsiveness to patients.

Methods Used to Address Downtime Data Needs

Typically, when technology is not working, we have to revert to traditional means for getting tasks done. It's the same whenever a healthcare information system goes down — clinicians have to record patient information on paper and periodically print out reams of critical patient records that they will need during a downtime. Both tasks are time-consuming. Printing records in particular can take a couple hours per day.

However, even if patient records have been printed out, getting access to the most up-to-date patient information, such as medication administration records and physicians' orders, can still be a challenge. The paper may have been printed in the computer room and be inaccessible to many of the users. A major issue is how unwieldy paper copies are to find the information that's needed from them, as there are typically multiple reams of paper printed.

Most importantly, even organizations that have backed up power, parallel systems and redundant solutions to provide data from their healthcare information system cannot know and ensure 100% that it is the *most recent* data.

ENSURING BUSINESS CONTINUANCE

Given all the possible issues and challenges presented above, one can see that business continuity planning is a good practice for healthcare organizations. Hospitals are a cornerstone of a community, so it is incumbent that they remain open and fully operational through any disaster, outage, etc.

To prepare for any downtime, you need to determine your Recovery Time Objective (RTO) and Recovery Point Objective (RPO). RTO refers to how long your organization can survive without this critical business function. Is it just the current day, until tomorrow or until next week? Also, what resources are needed to ensure the restoration of the function within the RTO?

RPO refers to data-reliant processes and how current your data needs to be once systems are restored. Is it last night's backup, or the last action taken? And, if you have a manual backup system, how long is it feasible to run the manual backup before restoration is impossible?

You may have complete downtime policies and procedures in place, but do you have a system that can automatically respond to an unexpected downtime and keep your organization fully functional until normal operations resume? Do you have a system that can provide your staff with access to the most up-to-date patient information plus meet requirements for patient data security and the need to ensure patient safety?

WHITEPAPER

The Solution for Downtime Data Protection and Business Continuance

NetSafe from Interbit Data is a downtime protection and business continuance solution that automatically captures and preserves critical patient information generated by your healthcare information system at regular intervals. The captured data is sent to and stored on local workstations, so the most recent patient information is available in the event of a network or power outage or other system downtime.

NetSafe scans the data for locations to ensure it is sent to the appropriate workstations in areas such as nurses' stations, admissions and the pharmacy. Running on battery-powered laptops or emergency generator-connected workstations during a power outage, NetSafe has up-to-date patient data at-the-ready – where it is needed.

With NetSafe, healthcare organizations can eliminate the need for continuous printing of patient reports, substantially reducing paper usage. Having up-to-date patient information available ensures the consistent delivery of quality patient care, even when your healthcare information system or network is not available.

During a planned downtime or the nearly inevitable unplanned incident, NetSafe serves as a de-centralized, up-to-the-minute stand-alone proxy system for your critical healthcare data. By polling your healthcare information system for new data on a recurrent basis, NetSafe ensures your staff always has the latest information at their fingertips wherever and whenever they need it.

NetSafe is cost-effective and easy to install. A typical NetSafe installation more than pays for itself within the first few months of service and can be up and running in under 8 hours. Given the costs of downtime outlined above, you would have a speedy return on your investment, along with the assurance that patient data, and especially patient care, is protected during downtime.

Conclusion

Your healthcare information system is entrusted with housing the most precious data in your organization — your patient records. Studies have shown that downtimes are inevitable and the frequency and duration of downtimes is enough to impact business continuity and your bottom line. System downtimes also compromise the security of your patient data. Most important, however, is the impact downtimes cause to the delivery of patient care. You have invested greatly in acquiring you information systems and training your users to rely on them. You have policies and procedures in place that address downtimes, but do they include the use of an automated system that captures a snapshot of the most up-to-date patient data at frequent intervals?

About Interbit Data

Founded in 1997, Interbit Data helps healthcare organizations deliver better, more consistent patient care with secure, reliable and cost-effective software solutions that improve operational efficiency. More than 750 customers worldwide use Interbit Data's products for secure information distribution, automated message delivery, and downtime protection and business continuance. For more information about Interbit Data and its products, visit the company website at www.interbitdata.com.

CONNECT WITH US

251 West Central St., Ste. 36, Natick MA 01760
508.647.0013 | www.interbitdata.com