INTERBIT DATA

Software to Improve
Healthcare Efficiency

WHITEPAPER

Insurance against Downtime in the World of Advanced EMR

The stage is already set for advanced use of online clinical systems; many hospitals are already using or implementing Electronic Medication Administration Records (EMARs), online documentation in nursing and, in some stage of implementation, Provider Order Management. As the details of the economic stimulus package that relate to healthcare IT are clarified, healthcare organizations will be encouraged to more aggressively implement and use these systems.

Although this advanced use of technology appeals to physicians, nurses and ultimately the patients, hospitals are now dependent on critical technology such as health care information systems (HCIS) for patient diagnosis and treatment, making it intolerable when systems become unavailable during a network failure or unplanned downtime. Physicians specify downtime as their top concern when contemplating the adoption of Electronic Medical Record (EMR) technology, as unplanned downtime has serious financial consequences due to the halt in operations and can negatively impact the hospital's ability to provide quality care. It is important for healthcare organizations to ensure that they have the ability to access critical patient information 24/7 and maintain continued operations and uninterrupted patient care.

While some downtime can result from weather or natural disasters, most downtime occurs because of security breaches, hardware or application failures and human errors. What comes as a real surprise is that planned downtime caused by routine backups, system upgrades and other activities planned by the IT department creates more than 70-90 percent of system interruptions. Regardless of whether it is planned or unplanned, downtime is inevitable and can be very costly to your organization.

What comes as a real surprise is that planned downtime caused by routine backups, system upgrades and other activities planned by the IT department creates more than 70-90 percent of system interruptions.

Planning for Downtime

Those healthcare organizations in the forefront of technology are already positioning themselves for these realities, ensuring their infrastructure can accommodate the new loads and capabilities. Additionally, they are working to stay on track with HIPAA's requirements for a contingency plan to respond to emergencies pertaining to access to electronic personal health information (PHI) records.

No matter how well you plan, there is no way of guaranteeing zero downtime. With more and more hospitals depending on electronic patient information as a norm, the amount of downtime that does not impact patient care is shrinking rapidly. Without access to the most up-to-date information available, downtime is more than a minor annoyance – it can be a life-threatening event.

Hospitals have put together plans and acquired products to recover from a major disaster, but what about the hiccup?

– What about scheduled downtime?

– What about a local network outage?

– What about a WAN failure to networked sites?

Even though downtime for planned hardware maintenance and backups is the cause of most service interruptions, hospitals need to plan for downtime that can occur for any length of time — from just a few minutes to a few hours or a few days — so that there is as little impact as possible. When it comes to downtime, the typical steps taken are:

- Eliminate downtime through redundant and fault-tolerant configurations;
- Ensure backup and data integrity through automated real-time and off-site back-up procedures; and,
- Build or contract for an alternate site to which operations can be moved in case of "disaster."

This process is essential for conditions in which power is cut off or property is damaged. Fortunately, systems are not required to respond because of these conditions very often. However, if there are departments in the hospital that are compelled to regularly print reams of reports "just in case," the concern clearly exists for a remedy beyond such contingency actions.

Selecting a Business Continuance Solution

Business Continuance, in contrast to Disaster Recovery, is an organization's ability to keep vital business operations running at or near normal capacities in the event of network or system downtime, whether planned or unplanned.

A scenario requiring Business Continuance is one in which the majority of the infrastructure remains in place and functional but it is unable to properly support the organization.

There are several solutions available for maintaining business continuance, ranging from printing backup reports periodically to totally redundant systems that can help healthcare organizations remain functional during periods of downtime. Organizations need to determine and select the appropriate solution based on their requirements, budget and needs.

Redundant or Fault Tolerant Systems

Most hospitals deploy hardware solutions to guard against unplanned downtime due to system failure or power outages. Even though buying additional hardware can be costly, redundant or fault tolerant systems are a necessary part of a disaster recovery plan when people's lives are on the line. Fault tolerant systems combined with battery backup or UPS systems can keep computers running and available.

In addition to being costly, this type of solution has a downside when it is the only one an organization is depending on for business continuance. What if the network gets disrupted and the HCIS cannot be reached to access the data in the first place? What if access to this data is dependent on the Internet because you are in another facility and that service is interrupted?

Printing Reports

One solution to intermittent downtime situations is to develop scripts that periodically create and print patient information reports as a backup in the event the hospital personnel are cut off from the systems that house the critical information. The benefit of having hardcopy reports available is evident during a total power outage, because you have the latest information on patients and are able to continue to provide appropriate care. Paper copies of patient reports may seem like a logical solution and may help clinicians and physicians feel more comfortable knowing they have a backup, but it does have its downside — printing reports in the event of a network outage just wastes time, resources and money.

Although the printing can be automated, someone has to retrieve the reports, organize them so that the necessary information can be found, and secure them from unauthorized persons. This activity keeps personnel from performing other tasks that may be much more critical to operations.

Printing reports not only increases usage of paper, ink and printer resources, it also increases costs due to the need to shred these sensitive documents prior to recycling. These costs will only increase in the future as the campaign to reduce waste and protect the environment gains strength. Supporting green practices is beneficial for hospitals as it helps lower energy bills, reduces waste and allows their environment to be more conducive to healing.

Although printed reports are valuable if you have a total power outage, printing reports in the event of a network outage increases the potential of unauthorized use and simply wastes time, resources and money.

Intelligent Report Generation and Distribution

Ideally, a business continuance solution should enable healthcare organizations to do the following:

- Identify critical information and automate its distribution to the appropriate locations where it will be needed in the event the HCIS is unreachable;
- Ensure the information is secured but available on local machines;
- Maintain seamless operation in the background, notifying operators of any interruptions; and
- Eliminate the storage of data in paper form, saving paper, ink, and printers, but still allowing the data to be easily accessible.

A downtime solution based on intelligent report generation and distribution provides an automated process. Such a solution decentralizes data in the event of downtime, allowing reports to be scheduled to print from the HCIS to the system and creating databases in multiple locations. These databases contain up-to-date versions of critical patient records, such as EMARs, and are secured via encryption. Information within the databases is indexed so that clinicians can search and find the information they need whenever they need it.

By ensuring access to critical data during periods of system failure or extended downtime, healthcare organizations mitigate risks to patient care and safety. When healthcare providers can depend on getting the information they need when they need it, they no longer encounter challenges to treating their patients. In addition, patients can be assured their health information and medical records are up-to-date and they are receiving the best possible care.

Conclusion

Clinical automation systems are no longer a luxury in the care delivery process; healthcare providers need them to achieve optimal efficiency and secure patient information. Ensuring that the information housed within an HCIS is preserved and continually accessible in real-time is important for maintaining a healthcare organization's reputation for providing consistent patient care. Because systems have a tendency to go down at the most inopportune time, having a software solution that ensures the 24/7 availability of up-to-date data, providing critical information where as well as when you need it can make a substantial difference in terms of protecting an organization's business and patient safety.

NetSafe – Continuous Access to Critical Information

NetSafe, a business continuance solution offered by Interbit Data, provides intelligent report generation and distribution. NetSafe automatically captures and preserves patient information and reports from the HCIS and stores it on any location on the network, making critical data available for lookup, review or printing whenever needed and ensuring consistent delivery of patient care when systems are unavailable due failure or downtime. Data elements can be automatically extracted from the captured reports and the reports are stored at locations throughout the network at regular intervals to ensure the most recent patient data is available. Data is encrypted to maintain confidentiality.

With NetSafe, users can define and capture an unlimited number of reports and rules, scan reports for locations to automatically deliver data to the right location and recipient, and store data at an unlimited number of locations throughout the network. Data is indexed for easy access to specific information. With the ability to send reports to multiple locations, healthcare organizations can ensure data availability and improve staff efficiency. Users can view report data online, removing the need to print the reports, and they can search reports for individual patient data. NetSafe possesses a comprehensive logging capability that allows users to create an audit trail and stores logs of all reports on a central server.

About Interbit Data, Inc.

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. Interbit Data was named to the Inc. Magazine list of the 5,000 fastest growing private companies in the United States. The company ranked No. 2909 as a result of achieving over 96% growth from 2005 to 2008, a growth rate that is 70% more than other companies in the same industry. Interbit Data products are used by more than 650 healthcare facilities worldwide. For more information about Interbit Data and its NetSolutions products, visit the company Website at www.interbitdata.com.