everbridge®

Reducing EMR and Clinical System Downtime

An Everbridge White Paper

Introduction

The majority of hospitals and large physician practices have implemented electronic medical records (EMRs) along with other clinical software systems. Healthcare providers are more dependent than ever on the performance of their information technology (IT) infrastructure. An IT failure can cause significant disruption at a hospital, making it impossible to access patient charts, process prescriptions or evaluate laboratory results and x-rays. Those failures have a hard dollar cost and potentially put patient safety at risk.

IT staff in the healthcare setting have to be able to quickly assess and address hardware and software failures, data breaches and other issues. They also have to rapidly communicate the nature and duration of these problems to upper management and the clinical staff that depend on these systems to do their jobs.

However, many facilities rely on outmoded paging systems, contact sheets and phone calls to address critical IT incidents. Valuable time is wasted just trying to locate and communicate with the appropriate staff members, which can extend the duration of these failures unnecessarily.

This white paper will outline the risks and costs of critical IT failures in the healthcare industry, and explain how a centralized electronic alerting and communication solution can accelerate the resolution of these problems, while saving costs and improving patient safety.

The Cost of Healthcare IT Failures

When important technology systems fail at a hospital, clinical operations can grind to a halt. In the last few years, National Nurses United, the largest registered nurses' union in the U.S., has criticized specific hospitals' use of EMR systems because these solutions can experience significant downtime and failures. Those criticisms have come in the wake of several high-profile IT incidents at major hospitals.

In 2015, nurses at Antelope Valley Hospital in Lancaster, CA, asked the Los Angeles County Department of Public Health to investigate an EMR failure that left doctors unable to review lab results, verify physician orders or access patient records for several days.

The overall **average cost** of a data center **outage** is **$690,204** per incident.

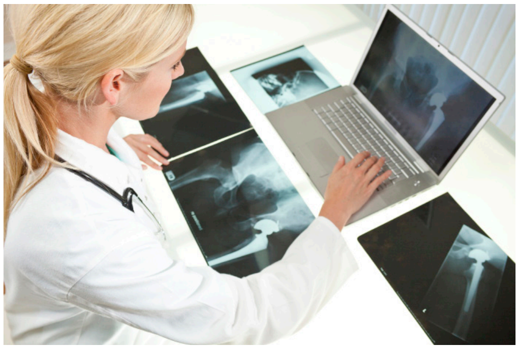
Rideout Memorial Hospital in Marysville, CA, experienced a similar outage when a burned out heating unit at an off-site data center left patient records and e-mail systems inaccessible. At Community Health Systems, a multi-hospital system with locations in 29 states, a data breach resulted in hackers stealing 4.5 million patient records in 2014.

Operational failures such as these waste as much as 10 percent of caregivers' time and can compromise the quality, timeliness and efficiency of care delivery, according to a working paper published by the Harvard Business School in 2013 (*Organizational Factors that contribute to Operational Failures in Hospitals*).

In addition to disrupting clinical operations, these crashes and breaches can cost hospitals millions. In the Ponemon Institute's 2014 Cost of Cyber Crime Study, the research firm found that the mean annualized cost of a security breach for the companies surveyed was $12.7 million per year. Ponemon's 2013 Cost of Data Center Outages study, meanwhile, found that the overall average cost of a data center outage is $690,204 per incident. Unplanned data center downtime cost healthcare organizations $627,418 per incident in 2013.

The longer it takes to resolve these incidents, the more costly the failure becomes. In hospitals, these IT failures can create dangerous conditions in which clinicians are unable to access critical patient information and medical devices fall offline.

All hospitals have disaster recovery plans in place in the event of a system failure but in order for those plans to be followed — for clinicians and pharmacies to revert back to paper forms, for manual checks of medical devices to take place or for staff to potentially relocate patients if critical systems become inoperable — staff have to know that an outage has occurred, how severe it is and how long it will last. For the incident to be resolved quickly and effectively, the right support staff have to be alerted, and they need to know important details about the nature of the outage in order to correct it.



But most of the time spent resolving an IT failure doesn't involve the technological fix at all. The bulk of the time it takes to achieve resolution is spent alerting the correct staff members about the failure, and then communicating with those staffers to ensure that the right people have responded.

According to the Ponemon Institute's research, the primary barriers to effective breach response include poor communications, lack of leadership and a lack of board oversight. Less than half of respondents (47 percent) said they were informed about the organization's incident response plan.

The overall Mean Time To Repair (MTTR) the outage or address a breach is impacted significantly by what is referred to as the "Mean Time To Know" (MTTK): the time spent alerting everyone that an incident has occurred in the first place, figuring out who needs to fix the problem, what teams are involved and how to reach out to those team members and receive acknowledgements.

The logistics of communicating with the key employees bogs down the process. Contacts or on-call information may be held in large spreadsheets. Telephone calls go unanswered or e-mails get missed. In a crisis, these communication hiccups can lead to catastrophic delays.

The Value of Unified Communications and Alerting

For hospitals to effectively address critical IT failures and data breaches, staff need a way to quickly communicate the right messages to the right staff members. They must be able to reach the right people quickly and collaborate easily.

Depending on the type of disruption, the communication necessary to resolve an IT failure goes beyond just the IT department. Alerts and instructions may need to be issued to senior executives, public information officers, clinicians or even transportation managers.

Without an automated, unified communication solution, just getting the right people onto a conference call to begin resolving an issue can take upwards of 30 to 45 minutes in some organizations. A unified critical communications and alerting platform allows companies to easily issue mass notifications, as well as targeted communications across multiple modalities (text, e-mail, phone, pager, etc.) to ensure key staff have all of the information they need to respond to an incident.

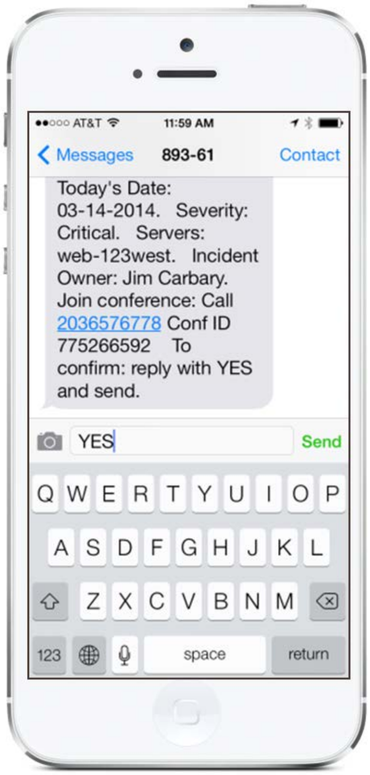
A unified communication and alerting system can provide a centralized repository of contact details for the resolver teams (IT staff, web services, application server experts, etc.), managers, customers, vendors, end users and other stakeholders. Such a solution can enable you to:

- Alert staff at multiple locations simultaneously and reliably
- Target alerts to affected users based on location, application use, software version and operational role
- Alert staff using a multi-modal approach that supports new and old technologies (phone, pager, text, e-mail, etc.)
- Develop automated follow-up alerts and escalations through integration with existing service management and monitoring solutions

These communications platforms not only allow you to reach out to the right people quickly, but to specify notifications so that, for example, key users of a specific version of a software system in a certain geography can be informed of an outage without bothering unaffected users in other regions with unnecessary alerts. In a hospital setting, where "alert fatigue" can lead to users missing or ignoring messages, this type of targeted messaging can be highly effective.

Staff members can be contacted via preferred methods, including phone, pagers, e-mail or text. The alerting platform can be configured so that if a message doesn't receive a response, additional alerts can be issued. Escalations can be managed automatically, with additional alerts and messages sent to supervisors and other staff to ensure a rapid response.

On-call schedules can be integrated into the alerting solution so that administrators can alert the right staffers based on the time of day and skill set required to address the outage. Doing so manually can waste time and increase the cost of the outage.



Today's Date: 03-14-2014. Severity: Critical. Servers: web-123west. Incident Owner: Jim Carbary. Join conference: Call 2036576778 Conf ID 775266592 To confirm: reply with YES and send.

YES

Such a communications platform can also provide an audit trail to help determine who was contacted, when they were contacted and how many times the system attempted to alert them before receiving an acknowledgement. That makes objective data available that can be used to evaluate any breakdowns in the response plan, measure performance against the plan and evaluate alternatives.

Leveraging an integrated unified communications and alerting platform will allow hospitals and other healthcare organizations to send both mass and targeted notifications and alerts during critical IT incidents. By streamlining and automating the alerts and escalations, healthcare users can accelerate the resolution of these critical incidents, potentially saving hundreds of thousands of dollars in the process.

Communication failures are a common frustration, and a leading cause of extending the duration of — and damage caused by — data center crashes, breaches and application failures. A central, automated alerting system can help healthcare providers maximize IT system uptime, improve employee productivity, reduce the mean time to repair IT incidents, boost employee morale, and most importantly,

About Everbridge

Everbridge is the leading unified critical communications platform trusted by corporations and communities of all sizes that need to reach the right people for immediate action, collaboration, and decision-making. Connecting more than 100 million people and internet-connected devices, the company provides reassurance that secure, compliant messages are delivered, locally and globally, received and responded to, no matter the recipient's location. Everbridge is based in Boston, Los Angeles, San Francisco, Beijing and London. For more information, visit www.everbridge.com, read the company blog, http://www.everbridge.com/blog, and follow on Twitter and Facebook.

THE ONLY END-TO-END PLATFORM

- **Everbridge HipaaChat:** Use Everbridge HipaaChat to quickly send secure messages, patient information reports, images or conduct telemedicine calls without incurring HIPAA violations.
- **Mass Notification:** Use Mass Notification to reach clinicians and employees about emergency situations and mass casualty events – across smartphones, email, SMS, push notifications and other modalities.
- **IT Alerting:** Use IT Alerting to help you restore system outages and quickly keep internal and external stakeholders informed.
- **Incident Management:** Use Incident Management with pre-defined notification procedures to speed up STEMI alerts and notify necessary hospital personnel faster to ensure patients receive life-saving treatment in record time.
- **On-Call Scheduling:** Use On-Call Scheduling for real-time shift calendars and integrated on-call notifications to automate the tedious process of contacting off-duty staff.

Visit www.everbridge.com to learn more.