White Paper **WP083030EN** Effective April 2017

Infrastructure best practices: Ensuring always-on power and availability for healthcare information technology

Justin Carron
Eaton

Executive summary

The healthcare industry is becoming more digital by the day. Central to this shift is the implementation of integrated healthcare information technology systems that replace legacy or poorly integrated systems. Today, healthcare organizations are striving to reach seamlessly integrated systems highlighted by Electronic Medical Records (EMRs) – one centralized component is the design to connect all stakeholders and systems, ranging from primary care physicians and specialists to hospitals, walk-in clinics, pharmacies and labs. The promise of integration and centralized applications is compelling: a significant improvement in the patient experience as well as better overall patient outcomes in addition to improved quality and decreased costs. With integrated robust and scalable IT infrastructure providing the foundation for collecting and sharing data in an EMR, healthcare will be transformed. Isolated silos of information and applications that were beset by inefficiency, inconvenience and errors will vanish. In their place, accurate applications will seamlessly integrate into centralized software. The vision is attainable, unfortunately not all healthcare organizations know how to do it.

As healthcare providers have implemented integrated EMR systems, the paperless world challenges have become apparent. While integration is good for patients and providers alike, it places a new burden on doctors and nurses as well as IT operations and facilities. A shared infrastructure tying together various stakeholders reveal issues like interoperability, continuity, security and availability take on mission-critical importance. In addition, security requirements are heightened due to the centralization of patient data – data that includes social security numbers, home addresses and insurance account numbers, making the data more valuable to hackers than credit card numbers. Stolen patient data can be worth more than $360, according to the Ponemon Institute.[1]

Shared data can improve healthcare, yet implementing EMRs is only one aspect of a comprehensive digital transformation plan. To truly transform healthcare, organizations must devise comprehensive strategies for their IT infrastructure that encompass resiliency, power management, availability, backup, security, compliance, scalability and growth. Such strategies should not begin and end with the data center but must also include every area where information is generated, shared, transmitted and stored. This includes computer rooms and networking closets, and spans to medical devices, network edge devices including switches and routers and the cloud as well.

Note: [1] See Hackers Selling Healthcare Data in the Black Market, http://resources.infosecinstitute.com/hackers-selling-healthcare-data-in-the-black-market/

Powering Business Worldwide

Abstract overview:

The ongoing transformation of IT in the healthcare industry is a reality. There are many benefits to adopt an integrated EMR system, but you also need to be aware of pitfalls. This paper outlines best practices for healthcare organizations to ensure a continuum of care across all stakeholders. This paper also highlights the need to build out a power management strategy across all facilities that contain IT equipment, while providing actionable advice for organizations that both own and operate their own data centers and those that maintain their infrastructures in a hybrid or hybrid cloud colocation environment.

Introduction

The shift to integrated healthcare IT systems began a decade ago. Since then, legislation has propelled healthcare organizations to replace cumbersome paper-based processes and legacy systems with integrated digital systems. Such legacy systems were in dire need of an overhaul; many systems were not fully automated, nor designed to be used across a system of stakeholders. As a result, patient data often was re-entered, duplicated and contained errors as it was passed along from one system to the next. Repetitive data entries were inconvenient, inefficient and error-prone.

Centralized EMRs are designed to allow various and disparate stakeholders both internal and external to a healthcare system access to comprehensive and up-to-date patient information. This holistic approach is critical in order to connect healthcare systems with external third parties such as pharmacies handling prescriptions and insurers handling payments. Unlike the standalone legacy systems, centralized EMRs are deployed with collaboration and information sharing in mind, and consequently are not designed for specific stakeholders. Manual paper-based processes can and should be replaced with automation that seamlessly facilitates workflow. Accurate and updated patient data is accessible throughout a healthcare system, enabling a single and unified view of records to all stakeholders that require access.

There are many significant benefits that healthcare organizations and patients can realize with a centralized EMR. Among the chief benefits of these systems: they allow doctors to see more relevant information in one place, better track patients over time, and share information with patients online. EMR software also includes safety features to prevent doctors from prescribing medications that could interact with one another and cause harm. These benefits result in a higher quality of care as all stakeholders have the information they need in a timely and accurate fashion. Automation and a reduction of manual processes both reduce errors and decrease fraud, particularly in areas such as prescriptions. Reduced data entry requirements, centralized records management and storage improve administrative efficiency as well as compliance efforts. Patients stand to experience additional benefits — they can quickly and conveniently access their own medical records and can better communicate with their caregivers.

The benefits of integrated healthcare go beyond more efficient operations. Having a huge amount of patient data readily available throughout a network allows healthcare providers to enter the era of big data, analytics and tele-health. Mining both historical and current data to discover patterns can lead to all sorts of actionable information affecting everything from staffing levels and clinical research efforts to facilities management and – ultimately – better patient outcomes. And having better outcomes will lead to better business results as healthcare providers are compensated for the quality of the care, not the volume of procedures. While the business case for modernizing healthcare IT is compelling, transferring information to a digital interface took time to do it right. Incentives were still needed to encourage healthcare organizations to invest in IT. Over time, various pieces of legislation such as the Health Insurance Portability and Accountability Act or HIPAA, the Affordable Care Act, and the Health Information Technology for Economic and Clinical Health Act – have evolved to the point that the adoption of electronic medical records is now mandated. In conjunction, government grants and financial incentive programs around Meaningful Use were formed to enable smaller healthcare organizations to adopt EMRs. Large healthcare systems – with their distributed networks of operations and significant financial resources – led the charge. As a result, these larger organizations are ahead to the curve in terms of the implementation of integrated IT infrastructure and centralized EMRs.

The adoption of centralized EMR implementation is encouraging. According to a report from Kalorama Information, the market for EMR systems has surpassed $26 billion, showing the increased investment in implementation. The Healthcare Information and Management Systems Society (HIMSS) tracks the adoption maturity levels of EMRs. At the end of 2015, more than 77% of 5,460 hospitals tracked in the United States have developed significant digital capabilities due to their level of EMR adoption.[2]

As implementation of EMRs expand, so too will demands on the IT infrastructure that supports those systems. These new systems need to be equipped to grow and flex with the population and age of a facility. In addition, they need to be resilient. Downtime is not an option when medical records are on hand. Currently, 30% of data worldwide is healthcare and the amount is only going to increase. Genomics research, medical devices and EMRs will result in a quadrupling of data storage requirements every three years.[3]

Challenges of implementing or updating an integrated healthcare IT infrastructure

The information sharing and seamless communication made possible by centralized EMRs are only as good as the IT infrastructure that supports them. With a holistic IT environment, planning, modular/scalable systems, storage and security take on added importance. If any part

of a healthcare system network is down, stakeholders are impacted. Information can become inaccessible and proper care can be delayed – a scenario that isn't an option for critical care organizations. In addition, as enterprises become increasingly dependent on infrastructure to ensure ongoing operations and drive business results, downtime is no longer an inconvenience; downtime now has significant costs.

Regulatory compliance poses another issue. For a large healthcare system, compliance is a significant challenge given the distributed nature of operations. Medical records must be safeguarded for privacy – a daunting prospect when records are shared throughout a system and must be stored for years. Providers and payers that violate regulations such as HIPAA are subject to steep fines depending on the severity, intent and scope of violations. Fines range from a minimum of $100 for each violation and $25,000 annually for repeat violations, up to $50,000 for each violation and $1.5 million annually for repeat violations. Keep in mind that monetary fees are only one aspect of penalties healthcare organizations may face; a data breach often results in negative publicity, cost in issue resolution and damage to an organization's reputation.

Security is also a concern in the new model of healthcare IT. Healthcare data is extremely valuable, making it a primary target of cybercriminals. Healthcare records contain the most valuable personal information – such as full name, social security number,

Note: [2] See https://app.himssanalytics.org/stagesGraph.asp

Note: [3] See The Alarming Epidemic Confronting Healthcare: Big Data, http://www.eaton.com/FTC/healthcare/KnowledgeCenter/BigData-Infographic/index.htm

home address, phone number and employer. These valuable pieces of information are coveted by cybercriminals who use them to steal identities and perpetrate insurance fraud among other illegal and highly profitable activities. Recently, there have been high-profile cases of hospitals victimized by ransom ware – in which their computer systems are locked until they pay thousands in ransom.[4] Security concerns are also growing for healthcare organizations as they've typically focused on their primary business, providing patient care. As these organizations have not traditionally been IT-driven they have not devoted significant resources to cyber security. For these reasons, healthcare organizations are particularly vulnerable to cybercrime.

With cybercrime on the rise, healthcare organizations need to seriously consider the threats and associated expenses related to data breach mitigation and resolution. The Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data conducted by the Ponemon Institute (published in May 2016), concluded that data breaches in healthcare are increasing in terms of costs and frequency. Nearly 90 percent of organizations surveyed reported having experienced a data breach within the past two years; on average, healthcare organizations spent more than $2.2 million to resolve issues related to a data breach. Each of these breaches involved on average more than 3,100 lost or stolen records. For the healthcare industry as a whole, the Ponemon study estimates that data breaches are costing organizations $6.2 billion annually.

The reality is simple. This this threat is not going away. Also, ignoring the issue or paying your way out of an issue is not a long term solution. You need to think bigger. You need to get to the source with your system.

Implementing a new system also brings on additional costs that can seem overwhelming at first. These costs are extremely difficult for small and mid-size organizations and still pose problems to large conglomerates. Costs for implementation include software, training, licensing and consulting. It's important to realize that these financial strains are short-term as investments in new systems will pay dividends in the long run. Making the initial investment can be tough but it can ward off and solve future issues.

Power management for stakeholders: adopting a holistic strategy

When healthcare organizations transition from paper to paperless clinical processes, they need to have an overarching strategy for power management that is modular and scalable. Given the expansive scope of many healthcare organizations, an effective power management strategy enables organizations to track and reduce energy consumption while ensuring availability and reliability. A comprehensive power management strategy encompasses key locations across an organization – from data centers to computer rooms and wiring closets. This approach makes resiliency a top strategy.

Benefits of high efficiency UPS

To increase power management reliability, high efficiency UPSs are a key solution. Most modern UPS products offer high efficiency modes that can significantly reduce power demand and costs, without sacrificing reliability. A new UPS replacing an old unit can pay for itself in 2-3 years when in high efficiency mode. While larger facility UPSs will often exhibit the most impressive power savings, the contributions of smaller network UPSs add up as well. Additionally, the high-efficiency mode will reduce the radiated heat from any size UPS dramatically. This can be important within closely confined locations like network closets, where excessive temperatures can trigger an unexpected shutdown of the IT equipment. It is also important to note that UPS batteries are sensitive to heat; temperatures that average higher than approximately 90 degrees can cut battery life in half – a large, unexpected and frequently avoidable expense.

Modular and scalable UPS

A modular UPS is loosely defined as "a large UPS comprised of multiple smaller UPSs." This architecture provides inherent redundancy to improve availability without the need to procure an "extra" full UPS with batteries, and associated footprint and maintenance. The ability to scale these systems if and when required, increases the flexibility and longevity of the UPS solution, while reducing the tendency to "overprovision" the original installation. The organization can save Capex, reduce Opex while increasing availability. The benefits of a modular and scalable strategy apply wherever infrastructure equipment is housed, ranging from a single wiring closet, to a midsize computer room, up to the datacenter and the facility overall. Large scalable UPS products may have the ability to allocate their capacity in real time-based sensing of load levels. This capability improves power usage, while reducing wear and tear on mechanical devices like fans and electrical switches.

Power distribution equipment

Centralized and distributed power distribution, everything from switchgear and panel boards, to rack mount and floor based, are integral to the facility's day to day operations, safety, and emergency power systems. Thus it is often governed by regulations that dictate how it is applied, such as UL, ANSI, IEC, and NFPA. Modern switchgear systems offer reduced footprints, layout flexibility, enhanced safety features, while providing comprehensive communication and metering capabilities that enhance their function by warning when conditions degrade, or provide predictive analysis to optimize maintenance costs. Furthermore, standalone power distribution units, or PDUs, provide voltage transformation and distribution of critical UPS power to the data center equipment, while offering similar predictive capabilities for monitoring via both facility-friendly (Modbus, Bacnet), and IT- friendly (SNMP) protocols. When considering power distribution at the rack level, look for products that don't require professionals for installation or subsequent reconfiguration; such rack-level distribution products should be modular and easy for a user to install by snapping into a rack. Power strips – also known as ePDUs – can be much more than just a place to plug in IT gear. With color coding for balanced loading, ePDUs can provide self-monitoring over a network. Using the network, an administrator can gather specific information on every device that is connected to the power strip, and even arrange locked-up server re-boots, by cycling power to individual receptacles. All of the above features are valuable both in large data centers, and in smaller IT environments, where onsite monitoring and administration is limited; hence the need to accomplish these tasks by "remote control" which is now possible.

Virtualization software and integration

Since most enterprises use some level of virtualization, healthcare organizations may opt to exploit virtualization's full benefits – hence the need to tie virtualized systems into UPS systems. Healthcare organizations can certainly reduce equipment and footprint, yet that is just one advantage of virtualization. With virtualization, organizations can have the ability to migrate both data and processing power to remote locations or disaster recovery sites – all handled by the hypervisor, based on a trigger alarm from the UPS system which can occur during a power outage, or overload situation. The UPS triggers the hypervisor to initiate an automatic migration of virtual servers and data, which can be accomplished seamlessly, without requiring a shutdown of operations and subsequent re-start. No data is lost, and the process is transparent to the user.

Note: [4] See Ransomware Wreaking Havoc in American and Canadian Hospitals, http://www.newsweek.com/ransomware-wreaking-havoc-american-and-canadian-hospitals-439714

Comprehensive backup and power management

While a hospital may have emergency backup, it's necessary that all stakeholders including clinicians and ambulatory care have backup capabilities as well. Without this, critical systems and equipment will not work during power disruptions, thereby compromising the continuum of care. An overarching power management strategy that encompasses all locations where computing equipment is installed is required. This may include network closets, colocation data centers, network edge and the like. A central component of this strategy is airflow management through the utilization of containment, blanking panels, fan units, hot and cold aisle design, cabling systems among other techniques.

Best practices for meeting challenges and requirements

Given the various stakeholders involved in modern healthcare, there are a number of best practices that can mitigate the challenges that integrated systems can bring. Top of mind should be an overall metering and remote monitoring strategy that allows individual stakeholders to track energy usage and ensure availability across facilities as well as across devices. There are UPS management platforms and energy management systems that make remote and granular monitoring a reality. Such systems collect and analyze data from connected infrastructure devices, enabling ongoing monitoring and predictive insight – all from a single interface. In addition, these systems can enable IT administrators to manage power consumption at the device level and automate disaster avoidance while enabling regular preventative maintenance.

A power management strategy will serve to ensure that critical healthcare systems stay up and running. Among all stakeholders, it is important to ensure that they both receive and provide timely updates to patient data and EMR systems. In effect, stakeholders are charged to "keep the database current." In a similar vein, stakeholders should strive to utilize common formats for EMRs that can be accessed and shared by other authorized medical providers.

Keeping the power on is always important for patient safety but it's also important for record access. Consequently, healthcare organizations need to deploy and maintain a power backup or disaster recovery site, so data is not lost, and information can be accessed even during power failures or adverse environmental events.

For specialists and primary care providers, it's necessary to store the most recent patient records and data locally for temporary use, and back it up in a master database. Keep in mind that local providers still need the ability to care for patients, even if the remote data storage is inaccessible for any reason. Maintaining a "local" cache of recent patient information helps deliver continuity of care even if network communication is interrupted.

For primary care providers, having a disaster recovery plan or site is a best practice. Such a plan or site should be kept up-to-date with duplicate data and duplicate capabilities. To protect servers, storage and network gear in medical offices, UPS systems should be utilized. These power systems allow continual operations and save data during adverse conditions. Specialists as well can utilize UPS systems – and even a generator if required – to provide backup for medical imaging and medical lab equipment.

Backup power is also a critical component for edge devices such as switches and routers; consequently, backup power systems deployed in network closets and imaging labs can ensure that communications can function normally during a power event.

At the hospital level, backup power devices and generators should also be deployed. In the case of hospitals, such power backup deployments must comply with guidelines issued by the Joint Commission on Accreditation of Healthcare Organizations (JCAHO). In addition, hospitals should test generators and UPS systems on a regular basis – at the very least monthly. Within a hospital, life safety, operating suites, imaging labs, emergency lighting, HVAC and egress areas such as elevators all should have power backup systems.

For those healthcare organizations that operate outpatient facilities – where onsite IT support may be limited – the remote monitoring and management of UPS and power distribution systems such as ePDUs is a great way to improve patient care. Even though these facilities do not have surgery rooms and scanners, the patients have extremely specific care plans that need to be followed. When these care plans are digital, backup power is absolutely necessary.

To keep healthcare providers up and running safely, remote capabilities can allow for faster response time to repair of network or server problems. This allows IT personnel to access even the smallest data closets from the comfort of their own home. To implement remote capabilities, , healthcare organizations should consider this during the design phase of a facility whenever possible. For existing facilities, it's never too late to make modifications or upgrades to gain remote and modular access. Just keep in mind, these solutions should contain critical components such as UPS and cable management systems for easy user installation, modification, upgradeability and serviceability.

Healthcare organizations typically operate multiple distributed facilities. In these kinds of disparate environments, it is recommended to deploy management software that allows monitoring of critical systems from a central location – typically a location that is removed from the actual building where the communications and computer hardware resides. Another deployment option for management software is within private cloud environments. Ideally management software provides predictive data analysis, so the user is notified in advance when things – such as when a UPS failed its battery test or a power distribution device is detecting intermittent overloads – are trending downward. This predictive analysis in turn allows IT administrators to take proactive action before a more serious issue develops.

In laboratories, sensitive equipment, such as blood analyzers, test devices, and so on, should have backup power, as well as the ability to save data if a power event occurs. Pharmacies as well should have similar backup capabilities with the addition of automation and recordkeeping equipment.

Battery backup times and generator fuel supplies should be chosen/modified, based on local weather conditions and climate. Healthcare organizations need robust functioning battery backup systems. Even in that event, having a "plan B" if a power outage is extended or the generator doesn't start is a necessity. Hence, there is always a need to plan ahead. A professional to help guide you with these decisions is always helpful.

Location-specific best practices

In data centers, UPS and generators are certainly a must. It is also important to test by simulating a power failure to ensure that everything is connected to backup power and that the backup functions normally within the specified battery backup time. The backup capabilities should encompass older equipment, network and communications gear, newly installed or temporary servers, storage and communications devices. Try scheduling this with your monthly power tests to ensure this is top of mind.

Within network closets, UPS is required so communications can operate during power failures and weather events. Also consider AC power in any backup power plan.

Computer rooms as well should have all the power and backup capabilities as a data center and network closet. Keep in mind, however, that a computer room may be served only by the building's HVAC unlike a datacenter, which has dedicated and backed-up HVAC.

Consider the advantages of using a "centralized" UPS architecture – one UPS for the whole computer room – or a "distributed" UPS architecture, where multiple UPS devices are placed in individual racks. Of course, there are pros and cons for each strategy. In a centralized architecture, operating and installation costs are typically

higher. However, a single UPS and battery system is easier to maintain and monitor even if the room is dependent on a single system. If redundancy is required, this too is easier in a centralized architecture. In a distributed model, cost is lower and there is the added security of not being dependent on a single UPS. On the downside, managing and monitoring all UPS devices and battery strings can be daunting; it can be difficult to know if "all that backup hardware" is going to function perfectly during an outage. This may result in less peace of mind than a centralized system.

Security of course is needed to safeguard data and patient privacy throughout the healthcare system. To safeguard operations, healthcare organizations require resiliency, redundancy and power management.

Many large healthcare systems operate their own data centers. These facilities must have the redundancy and resiliency to keep operating during any contingency. Backup generators, backup batteries and UPS devices can provide the power infrastructure required for servers, storage and networking equipment. To better manage power across a disparate network, PDUs are important components. Throughout the networking infrastructure, gateways and switches can enable organizations to remotely analyze power equipment – a critical capability given the integrated nature of the new model of IT.

In network closets – offshoots of a data center that house servers, data storage equipment and switches – UPS and PDUs can provide remote monitoring and management of power usage, as well as keep tabs on important environmental metrics such as temperature and humidity. Computer rooms as well can benefit from UPS and PDUs in addition to cable management and racks that optimize the airflow, accessibility and organization of the equipment.

For healthcare organizations that opt to deploy a hybrid (comprised of on premise and cloud) environment or go with a collocated data center provider, it's important to ensure that the service provider can deliver a secure, resilient and reliable infrastructure. To this end, a provider should have a comprehensive disaster recovery plan in place; if one facility goes down, there should be multiple backup facilities that can seamlessly run any and all workloads. Make sure that the provider is able to adequately address HIPAA compliance requirements in terms of data privacy and data retention. On the latter point, scalability is a must with exponential growth of data volumes. A service provider must have the ability to scale to accommodate data growth, and in addition have the ability to expand bandwidth capacity to facilitate big data and analytics.

Conclusion

For healthcare organizations, EMRs in conjunction with an integrated IT infrastructure promise to improve patient care, reduce costs and increase efficiency. However, to achieve sustained benefits, healthcare organizations must take measures to ensure availability, scalability, resiliency and data security. With a well-thought out infrastructure strategy encompassing everything from power management, security and backup, and including all the various stakeholders, healthcare organizations can achieve all the benefits that the new model of integrated IT can offer.

Power management: questions to consider

Across the healthcare landscape, many critical systems are housed in network closets and computer rooms – small spaces that were not designed initially to hold heat-generating IT equipment. For these facilities, IT managers must consider the following questions when building a power management strategy:

- What will happen to your network closets, if the building's HVAC shut down?
- During power outgages, will there be a need for portable air conditioning, or least fans?
- In the event of an extended outage, what backup power options are needed for the network closet?
- When do you need to replace your batteries?
- When is the last time you've tested your system for power continuity?
- If the power goes out for three days, can your IT equipment still function with monitors across your facility?

Eaton
1000 Eaton Boulevard
Cleveland, OH 44122
United States
Eaton.com

Printed in USA
Publication No. WP083030EN /
CSSC-1611-3731
April 2017

Powering Business Worldwide