## Contents

1. Introduction
3. Exceeding Regulatory Compliance Requirements
4. Power, Operations and Emergency Response Coordination
5. Business Continuity Improvement Considerations
6. Enhancing System Availability
7. Technology Support of Critical Applications
8. Precision Control of Comfort and Environment
9. Sustainability and Energy Savings
10. Securing Buy-in from Executives
11. Additional Resources

## A Practical Guide to Ensuring Business Continuity and High Performance in Healthcare Facilities

Schneider Electric Reference Guide
Introduction

Within healthcare facilities, high availability of systems is a key influencer of revenue and patient safety and satisfaction. Three important critical success factors need to be addressed in order to achieve safety and availability goals. These include exceeding the facility’s level of regulatory compliance, a linking of business benefits to the maintenance of a safe and an “always on” power and ventilation environment, and a sensible approach to technology upgrades that includes new strategies for “selling” technological improvements to executives. This reference guide offers recommendations for identifying and addressing each of these issues.

The mission-critical nature of hospitals and healthcare facilities requires that stakeholders build their business around a philosophy of high availability of services.

The mission-critical nature of hospitals and healthcare facilities requires that stakeholders build their business around a philosophy of high availability of services. At the physical level this implies the design and deployment of data and power networks that support availability, business continuity, and disaster recovery goals.
Introduction (cont.)

and multiple procedures, standards, and rules to follow. In the event of actual damage from disasters, system restoration practices must also be clearly defined.

Healthcare facilities have exceptionally low tolerances for power disruptions. Minor fluctuations can impact the delicate voltage requirements of MRI and CT scanners, for example. More extensive power events can affect life support systems, as well as critical ancillary infrastructure systems such as HVAC, communications, records management and security.

A true disaster recovery strategy needs to be holistic. The plan must take into account how key facility systems interact and support each other. This includes the electrical architecture, the building management system, the heating, ventilation and cooling controls, lighting systems, the data center and hospital information system, security cameras and access control systems, medical equipment and modalities, and specialized systems for critical areas such as operating theaters.

As technology networks evolve, the ability to assure the availability of both business processes and the technology backbone that supports those processes becomes increasingly critical. Business specific trends within the healthcare industry, including an aging population, shrinking budgets, increasing patient population, growth of outpatient facilities, the need for actionable data, transition to digital and mobile technology platforms, regulatory compliance, prevention of healthcare-acquired infections, improved bed turnover, and the need for more hospital operational efficiency, are driving new ways of managing and adapting healthcare facilities.

New technologies have altered healthcare administration methodologies and the ways that patients access healthcare services. Consider the example of a local doctor who cannot solve a medical problem without the help of a specialist at a large metropolitan medical center located thousands of miles away. Connected technologies allow the specialist to see the patient on a screen, virtually via a diagnostic imaging device connected to the Internet, and the patient’s life is saved.

For this level of communications sophistication to work properly, a whole chain of elements has to interact flawlessly from one end to the other, and everything depends on power infrastructure. If any link breaks, that screen goes blank. The evolution of technology has transformed the way healthcare facilities conduct their business. Business continuity, disaster recovery and high availability are now tightly coupled with patient safety and satisfaction.

Increasing healthcare demands are driving new approaches to managing healthcare facilities.
How New Technologies Impact Business Processes

The environment of an “always on” infrastructure impacts the ability of a healthcare facility to adapt to marketplace shifts and to accommodate the higher service level expectations of patients. The following paragraphs identify and analyze the major business drivers that now demand a high availability facility, capable of safeguarding business continuity with robust contingency plans in place to enable rapid disaster recovery. For many healthcare facilities, the continued growth and profitability of the institution will depend upon a realignment of infrastructure to support the high availability goals.

Electronic Medical Records (EMR)
An avalanche of electronic patient data comes into hospitals and other healthcare facilities on a daily basis—registrations, examination reports, test results, images, billing, and communication with insurance firms are just a small example. Managing this data stream becomes more and more critical to a hospital’s reputation for efficiency and professionalism. Each year, hundreds of thousands of people die or suffer adverse effects as a result of inaccurate or incomplete medical records that can mislead a diagnosis and affect testing and treatment. Integrated and improved IT solutions can potentially cut this number in half by enabling more accurate and accessible medical records that can support the right medical decisions.

Electronic medical records make it essential for medical staff to have consistent, quick access to the IT system and also require reliable power for backup procedures and archiving. The rack systems, security, IT management software, and power and cooling within the data center that protect the servers and storage, are critical elements in supporting the medical records system uptime.

Some national governments have begun imposing financial penalties against hospitals and doctors that have failed to adopt electronic health records. However, what happens if electronic medical systems go down as a result of a power outage or natural disaster? The vulnerabilities of hospitals to outages increases exponentially, especially if backup plans are weak and lack the necessary infrastructure recovery details. Hospitals and healthcare employees could lose access to patient medical records for hours. In such cases, doctors and nurses have to revert to writing orders and notes by hand. New shifts of doctors and nurses coming into the hospital have no access to the historical patient data. The risk of making critical mistakes increases. The situation gets magnified during a natural disaster as the need for medical services increases as casualties from the surrounding area flood to the hospital. This is why federal law requires medical providers and their vendors to have contingency plans in place for when systems go down.
How New Technologies Impact Business Processes (cont.)

**Self-service tools**
More and more self-help electronic devices are making their way into hospital and clinic waiting rooms. These self-service kiosk strategies look to run healthcare more like the airlines or leading online retailers. Such devices are utilized for applications such as patient check-in, consent forms, co-pay collection, facility navigation, secure enrollments, scheduling, and pre-registration.

The UK’s National Health Service (NHS) is one example of a healthcare organization that has invested in self services. Among other services, NHS launched a health and symptoms checker, including a mobile app. The investment resulted in shorter wait lines, reduced congestion in emergency rooms, and cost avoidance from patients not visiting hospitals. According to Deloitte, estimated benefits are reaching £25 – 50 million annually.¹

In some cases, waiting rooms are being eliminated since patients can proceed directly to a care room. Rather than a patient having to visit a laboratory to have blood drawn, or to receive a shot, a mobile lab can serve the patient within the care room when needed.

Another self-service growth area, tele-consultation, provides individuals requiring services with the ability to work with physician’s assistants via tools such as Skype. This allows for much more rapid and less costly diagnosis of lower severity conditions.

Patients are encouraging providers to make more self-service options available for transacting healthcare-related tasks such as scheduling appointments, paying bills and filling out or updating forms. But as patients become more reliant on self-help kiosks, these new self-service tools will require the same high-availability levels as the more traditional core healthcare systems. With bill-payment kiosks, for example, if power is lost during the process, it can easily lead to a variety of problems including unconfirmed payments or the transaction not being submitted. One approach, from a backup and recovery perspective, is to integrate a portable uninterruptible power supply as a source of backup power. In such a scenario the kiosk user will have more time (the battery immediately begins to furnish the power the very second the power gets cut) to finish their transaction prior to the battery power running out.

**Radio Frequency Identification (RFID) and Real-time Location Systems (RTLS)**
These technologies are now being deployed to ensure the safety and security of the most vulnerable patients, such as infants, the elderly, and those with mental illness. These technologies provide healthcare facilities with the ability to

¹ Deloitte, “Connected Health: How Digital Technology is Transforming Health and Social Care”, Deloitte Center for Health Solutions, 2015
Radio Frequency Identification (RFID) and Real-time Location Systems (RTLS) are used to ensure the safety and security of patients.

How New Technologies Impact Business Processes (cont.)

...identify, locate, track, and monitor patients, visitors, staff, assets, and equipment. Typical return on investment for RFID/RTLS projects is 1 year or less. Value is maximized for both patients and the healthcare facility when this technology is integrated with the facility’s security, energy, building and power solutions.

RFID helps hospitals identify objects, locations, and people through the remote use of radio waves. Simple RFID devices use an identification system, such as serial numbers, to track and manage objects. Other more sophisticated RFID systems, such as the kind used in operating systems, have built-in sensors that communicate data on location for identification purposes and on environmental conditions. RTLS is used to identify and track the location of objects and people in real time, typically within a building or other contained area. The RTLS physical layer usually consists of some form of radio frequency, but some systems use optical (infrared) or acoustic (ultrasound) technology instead of or in addition to radio frequency. RTLS provides real-time tracking of people and physical assets with more precision, higher granularity, and a greater level of accuracy than RFID or other identification systems.

The application of RFID and RTLS technologies benefit hospital profitability and patient care in several ways:

- **Improving patient and staff safety**—RFID and RTLS help prevent patient elopement (e.g., a patient who wanders off unnoticed) through integration with access control, video surveillance, and other electronic security and building technology. Not only are patients and staff safer, but in many cases facilities are also realizing lower insurance costs. Typical RFID and RTLS applications include access control, emergency response, infant protection, patient management, and enhanced video surveillance.

- **Enhancing quality of care**—Facilities can also streamline and improve the quality of patient care by increasing efficiencies through reduced time and costs spent in locating assets, equipment, patients, and staff. Hospitals can implement RFID and RTLS applications for asset and equipment tracking and utilization, inventory and laundry management, and loss prevention. In fact, according to a study by Transparency Market Research, of all the applications where RFID is used in a healthcare setting, tracking medical hospital equipment accounts for the largest revenue generating application.

- **Reducing financial waste**—With RFID and RTLS, organizations experience less theft and equipment hoarding, as well as reduced rental and late return fees for important hospital equipment. Improved asset and
equipment visibility leads to improved utilization and often results in a ROI of less than a year, especially for the RTLS technology. Applications in this area include anti-counterfeiting, product authorization, and bed and operating room management.

Robotics

The average age of the elderly population is increasing, due to the ever increasing quality of healthcare. This trend will exacerbate the shortage of trained healthcare professionals such as nurses moving forward. The growth of robotics is one way in which new technologies will help to address this aging population issue. Although robotic technologies have been applied to the healthcare industry for a number of years, robotics represents a significant new growth area for enhanced services.

Robotic systems are very complex. They represent a convergence of human-machine interface designs, sensor systems, mobile energy supply, energy efficiency and biocompatible materials.

Robotic systems add value to healthcare enterprises in four major ways:

- **Reduction in labor costs** – On the logistics side (e.g., assembling proper medications for a particular patient) robots can replace specific human activities.

- **Increasing independence and social participation of vulnerable people** – This can lead to both social and economic benefits. An example is the ability of handicapped or elderly persons to feed themselves in an increasingly independent manner.

- **Increasing the quality of care** – Robots can outperform humans when it comes to executing certain repeat and high precision actions (e.g., automated bone cutters for hip surgery).

- **Performing activities that cannot be performed by humans** – In cases where human limitations are an issue due to size or precision requirements, robots can outperform human surgeons. An example would be micro capsules for taking internal body tissue samples.

Prevention, diagnostics, intelligent prosthetics and robotized motor coordination analysis and therapy offer other examples where robotics can play an important role.

In all cases, the “food” that keeps the robotics equipment alive and running comes down to the power infrastructure. Whether robots are directly powered from outlets or from recharging devices that enable the extension of robot battery life, the stability of the power supply is critical.

**Chapters 1-2 Takeaway:** Analysis of industry trends can serve as a blueprint for prioritizing investments.
Exceeding Regulatory Compliance Requirements

Government regulation plays an important role in safeguarding the health, safety and privacy of healthcare system employees and patients. Adherence to these regulatory drivers often determine the reputation and resulting success of a particular healthcare institution. Making an effort to exceed the regulations is a sound strategy for both enhancing the net worth of the institution and for preparing in advance for future regulations that may become more stringent. With an uptick in mergers, affiliations and integrations, how much a facility exceeds compliance can make or break a deal. As part of due diligence, hospitals need to evaluate the privacy and security compliance of the practice or provider they’re looking to acquire. Otherwise, hospitals may be taking on potential liability.

Regulatory compliance can be complex to track and fulfill. A sound, holistic healthcare facilities infrastructure supported by the proper electronic and electrical physical elements can simplify the process and significantly reduce the cost of compliance.

Across the globe, various national, regional and local regulatory bodies set standards for healthcare facility safety, quality of service, business continuity and disaster recovery practices. Listed below are some recommendations for how healthcare facility physical infrastructure best practices can help to supplement compliance to some of these key regulations:

Privacy and data security
The increased portability of electronic devices that store health information adds to the complexity of maintaining hospital security and privacy standards. Any individual can

Making an effort to exceed the regulations is a sound strategy for both enhancing the net worth of the institution and for preparing in advance for future regulations that may become more stringent.

Advanced security systems have to evolve as cyber-attacks increase in intensity and sophistication.
walk out of their office with confidential patient information on a flash drive, or laptop, and have these items stolen from their car. Therefore, vigilance, advanced security systems, and advanced compliance programs are essential for hospitals seeking to avoid investigation or liability.

Given the breadth of hospital staff and volunteers along with their access to electronic devices, hospital compliance efforts will need to go beyond a plan document. Hospitals should review their compliance documents, update them, conduct training of all their staff, and determine how often the hospital will conduct retraining. Hospitals need to be prepared for potential government audits.

On the data security side, critical infrastructures such as healthcare facilities are also becoming bigger targets for cyber-attacks generated from individuals, rogue groups, and nation states. These attacks are increasing in intensity and sophistication and are capable of changing system settings or destroying systems that are critical to our modern life. Water and power are particularly vulnerable to these types of attacks.

Network Intrusion Detection Systems (NIDS) perform preemptive analysis by searching for anomalies and signatures on the network. Once detected, an alert is forwarded to the analyst for review. Some NIDS also have a defensive capability (prevention) where they can block an anomaly or signature before it can cause damage.

NIDS are deployed at key entry points on a network and report their information to a central server where all alerts appear on a console. These servers tend to run an SQL database where alerting, signatures and reporting are stored. Cyber security analysts who are trained in viewing such alerts will be looking at network traffic to determine if the alert and signatures are legitimate attacks. In the event of an attack, appropriate action will be taken by the network defense team to resist the attack according to the organization’s internal process and procedures.

The extensive use of credit card processing in healthcare facilities also poses a risk of breaches in privacy. A recent report by McKinsey & Co. management consultant firm found that $45 billion worth of out-of-pocket medical expenses were charged on credit cards.² As a result, for the millions of people who utilize credit cards to pay for medical expenses, cyber security, identity protection, and privacy are significant concerns. Steps that healthcare facilities can take to address credit card security risks include the following:

• **Design and maintenance of a secure credit card network** – This includes the installation and maintenance of a firewall configuration to protect cardholder data, the avoidance of use of vendor-supplied defaults for system passwords, and the encryption of transmissions delivering cardholder data across open, public networks.

• **A vulnerability management program** – These types of programs enforce the use and scheduled updating of anti-virus software on all systems commonly affected by malware.

• **Access control measures** – Common practices include the restriction of access to cardholder data on a need-to-know basis, the assignment of a unique ID to each person with computer access, and restricting physical access to locations that house cardholder data.

• **Monitoring and testing of networks** – Here the focus is on tracking and monitoring all access to network resources and cardholder data. Security systems and processes are regularly tested.

• **Maintenance of an information security policy** – Efforts in this area are concentrated on documentation of the security policy and education of employees regarding policy procedures.

Credit card processing systems now require the same degree of high availability as do the core systems that support the medical systems within the healthcare facility. If a doctor’s office or accounts department has a UPS on site, it should be possible to continue to make electronic payments with a credit or debit card as long as the fixed network telephone lines still function.

How well a hospital pays attention to these privacy and security details will factor significantly into its marketability.

**Patient safety**

Patient safety is often affected by poor care coordination and poor communication. These conditions lead to an increased risk of suffering an adverse event. However, improvement of hospital work environments, a relatively low cost strategy that enhances safety and quality in hospital care, is a key driver of increased patient satisfaction. The rights and safety of patients and healthcare employees are enhanced if the facility infrastructure is designed with safety and simplicity in mind.

In facilities with x-ray machines, healthcare stakeholders need to identify the types of radiation used in the facility, and designate restricted areas to limit employee exposure. Employees and vendors working in designated areas should be asked to wear personal radiation monitors.

Safety-focused hospital work environments lead to higher levels of patient satisfaction.
In addition, radiation areas and equipment must be labeled and equipped with caution signs. From a power perspective, backup systems should be in place in case of power disturbance or power outage so that equipment can keep functioning at least until the issue is fixed.

Electrical hazards, such as wiring deficiencies, are best addressed through regular auditing practices. Design requirements for electrical systems and safety-related work practices should be reviewed every time new pieces of electronic equipment are added so that load balances are kept within safety ranges to prevent circuit overloads. If flammable gases are present, special wiring and equipment installation may be required.

**Disaster preparedness**
Any emergency action plan should include an emergency mode operations component. Such plans describe the actions employees and the patients in their care should take to ensure their safety in a fire or other natural disaster or power blackout emergency situation.

A facility that has established a reputation for safety builds the confidence of the local community that their local healthcare organization adheres to a high level of quality control standards. Vendors can help healthcare facilities enhance their reputation for safety and quality control through documentation of processes that support preparedness and safety should a disruption to business continuity occur.

In order to minimize the damage potential of disruption to operations, disaster preparedness plans should address these four critical aspects:

1. **Preparation and prevention** – Any set of activities that prevent a crisis, reduce the chance of a crisis happening, or reduce the damaging effects of a crisis. In the domain of power, for instance, a formal plan that describes backup procedures, generator testing, and UPS battery monitoring would be viewed as positives towards regulatory compliance and accreditation. In fact, in some countries like the US and France, performing periodic (monthly) tests is mandatory in order to secure accreditation.

2. **Detection and incident classification** – Actions taken to identify, assess and classify the severity of a crisis. In this case, an example would be a Building Management System capable of recording and documenting the severity of alarms as they pertain to temperature, physical security, fire, ventilation, water, and power supply.

3. **Response and mitigation** – Actions taken to save lives, prevent further damage and reduce the effects of the crisis. An example here would be a documented architecture of redundant power and cooling systems that will allow for business continuity and rapid crisis management.

4. **Reentry and recovery** – Actions taken to return to a normal or an even safer situation following the crisis.
Power, Operations and Emergency Response Coordination

In most geographical regions, hospitals must meet strict regulations in terms of tolerances for power interruptions to critical procedures and medical care zones. Codes seek to ensure that electric currents emitted from the various medical devices in a typical hospital room don’t harm patients. The more electronic devices that find their way into a patient’s room, the more difficult it becomes to comply with the standard. For example, it would not be appropriate to plug any old power strip into the wall behind a patient’s bed, then plug in a multitude of medical equipment.

At the same time, with the critical role that electronic devices play in patient care, healthcare providers need to ensure they are always on. Technologies such as Uninterruptible Power Supplies (UPS) are needed to keep systems up and running in the event of power glitches. When installing these devices, safety codes need to be respected. Proper installation requires the involvement of electricians and can be coordinated by either facilities or IT departments.

Within a hospital electrical distribution network, the circuits can be divided between the normal non-essential circuits and the essential electrical system. Non-essential circuits may not require an alternate power source, but the essential electrical circuits do.

Essential electrical systems

The essential electrical system includes circuits vital to the protection of life and safety including patient-care related circuits like the intensive care unit or operating rooms as well as emergency lighting, alarm systems, and battery chargers. Also included are all the electrical infrastructure equipment needed to ensure life safety equipment uptime.

Electrical power distribution systems cannot be designed and constructed to indefinitely operate. Assessments of the condition and maintenance of power systems can mean the difference between electrical code compliance and unanticipated power outages that cause business disruption.

Each country has its own installation standards, but in most cases, standards are based on the International Electro-Technical Commission (IEC), which clearly defines critical applications within healthcare facilities. IEC defines three critical levels and maximum duration times for power supply downtime. The tolerance depends on the power architecture of the healthcare facility and whether a generator serves as a backup to critical areas. A generator set takes approximately 10-15 seconds to fully power up, so a critical power system such as an uninterruptible power supply (UPS) must bridge the time between power outage and generator launch.

Many countries mandate specific compliance standards for generator testing and some require formal reports for government agencies and for audit purposes. These

---

Power, Operations and Emergency Response Coordination (cont.)

compliance standards may be mandated by national governments, local (state/provincial) governments, or by private organizations.

In the US, for example, hospitals are required to follow NFPA 99 and 110, which prescribe that Emergency Power Supply (EPS) systems have to be tested at least 12 times a year, every 20 to 40 days, for a minimum of 30 minutes at the manufacturer’s recommended exhaust gas temperature or at a minimum load of 30% of the generator set’s rating. Also, maximum transfer times of less than 10 seconds are typically required.

In Europe, IEC 60364-7-710 prescribes that changeover devices be tested every 12 months. Generator set combustion engines are to be tested monthly until rated running temperature is achieved with an additional 60-minute annual endurance test.

Hospitals are required to keep precise maintenance and test records for presentation to regulating authorities, or for traceability to determine what happened in the system after improperly functioning or system failure. In the case of system failure, despite proper testing, it is imperative to have access to detailed electronic data which facilitates sequence of event or cause and effect studies.

It is not uncommon for back-up generation to fail in the case of an emergency due to insufficient testing and maintenance. In some cases, nominal run tests can actually create problems within the generator sets that can affect operation in a true emergency situation (like wet stacking, where unburnt fuel or carbon builds up in the exhaust system when generator run times are too short or the test is performed outside recommended operating parameters). Comprehensive manual tests are difficult to coordinate and measured results are hard to achieve.

Emergency Power Supply Systems (EPSS)
In order to avoid this complexity, more hospitals are switching to automated Emergency Power Supply System (EPSS) test solutions. EPSS are designed so that one or more alternate power sources can supply the healthcare facility with power during an interruption of the main utility-supplied power. Typically, alternate power sources are made up of diesel or gas powered generators, sized to carry, at a minimum, any vital, critical and emergency loads. Power is transferred from the main utility supply to the alternate power sources using automatic transfer switches (ATS) whenever the main utility supply is interrupted. A facility may have one or several independent EPSS.
By installing an electronic system that continuously monitors and records EPSS-related parameters, it is easy to prove regulatory compliance, and have precise electronic records available for traceability and trouble shooting in case of an unanticipated failure. In addition, electronic records can be used for long-term EPSS trend analysis. Subtle long-term trends in parameters such as Automatic Transfer Switch (ATS) transfer-times, differential fuel pressure, and engine-start battery voltage can be used as flags for required maintenance. Automated testing and monitoring helps point out problems during testing rather than during an outage. As such, the system’s overall mean time between failures (MTBF) can be improved, giving patients, staff, and administrators peace of mind, so they can rest assured that the EPSS is ready to power the hospital whenever required.

During an emergency, and in between the time the power transfers from the utility to the generators, devices such as uninterruptible power supplies (UPS) and flywheels are used as a “bridge” to give the generators enough time to engage and warm up. UPS are connected to strings of batteries which make up the source of the stored energy that is reserved for these types of transfers and for shorter duration outages.

Flywheel storage systems, while generally higher in initial cost than sealed batteries connected to conventional UPS of equivalent KW ratings, have some characteristics which can make them desirable for some applications in the hospital environment (e.g., smaller footprint, effective management of short duration outages, less maintenance).

Some facilities may elect to run a Static UPS utilizing both a conventional battery and a flywheel storage unit in parallel in certain instances. The flywheel storage unit would protect against short duration events, extending battery life in the conventional UPS. This would be in place to provide an extra measure of protection for longer outages and full transition to generator power. It’s really a matter of being able to support the requirement for the particular facility, rather than forcing one approach.

In the healthcare market, the reality is that a range of UPS products are needed, from standby UPSs to protect nurses’ stations or PCs in offices, to single phase or three-phase solutions to back up medical equipment, operating theaters, intensive care units, and baby care units.

Chapters 3-4 Takeaway: Compliance and safety are a risk management issue. Infrastructure tools exist that help facilities exceed local and national compliance requirements to better protect their patients.
Business Continuity Improvement Considerations

When a 200-bed hospital experiences a power outage and its backup generator solution fails, the cost is $1 million – or $5 million for a 500-bed hospital. According to MeriTalk, an online government and healthcare IT community public-private partnership, 40 percent of global health organizations have experienced an unplanned outage in the last 12 months. The average cost is $432,000 per incident, and diagnostic imaging systems are among the leading culprits.¹

At the executive level, these risks are high and facilities and IT departments need to formulate a plan that reduces downtime risk and addresses both patient safety and cost avoidance. Revisiting the importance of infrastructure and facility management in healthcare plays an important role in assuring business continuity.

The average cost (of downtime) is $432,000 per incident, and diagnostic imaging systems are among the leading culprits.

Several possibilities that need to be considered are fires, floods, tornadoes or terrorism, hurricanes, hazardous material spills or human error, earthquakes, equipment failures, utility outages, and winter storms. At stake are people, property, information, the environment, and the well-being of the healthcare organization. In addition, other “collateral damage” like harm to institution reputation or liability that can far exceed the cost of lost equipment need to be considered. Disaster planning involves all measures taken to prevent, prepare for, respond, mitigate, and recover from a crisis.

In personal healthcare, the practice of routine physical exams for the early detection of disease is a highly successful method for the prevention of catastrophic illness. The same is also true for the prevention of a catastrophic loss when a physical or data security risk assessment is applied to healthcare facilities.

¹ MeriTalk, “Rx- ITaaS + Trust”, https://www.meritalk.com/study/rx-itaastrust/
Vulnerability assessment
Vulnerability assessment is the process of estimating disaster potential in terms of susceptibility to damage. A thorough vulnerability assessment should evaluate such crucial issues as the number of people at risk, the value of property, the number and function of the exposed critical systems, and the dangers of secondary hazards.

Risk assessment
The risk assessment is a measure that combines the likelihood of a hazard event with the probable degree of damage that would result. It should also account for secondary damage such as the ripple effects of rising temperatures on blood supply in a laboratory when a refrigeration system fails.

Disaster recovery assessment
Disaster Recovery addresses the adequacy of back up plans and procedures, equipment replacement prioritization, vendor lists, emergency response planning, plan exercising, and additional procedures that will expedite recovery from a disaster event.

Fire safety assessment
The most frequent cause of declared disasters is fire. Building fire codes are designed to ensure that structures are safe from fires for the occupants, and based on safe evacuation. However, an objective limited only to compliance to code is inappropriate. The various codes represent a minimum standard, and depending on risk and exposure additional measures should be considered. The key category in “learning before burning,” the Fire Safety Assessment focuses on fire safety systems (e.g., detector spacing and appropriate usage), hazards (e.g., paper and flammables storage), evacuation procedures, fire suppression, and fire department

Below are examples of some of the assessments that should take place as part of the business continuity plan:

Hazard assessment
Hazard assessment is the process of defining hazard-prone areas. These hazards can include wild fires, mudslides, tornadoes, hurricanes, railroads, gas lines, floods, etc. The hazard assessment estimates the probability and severity of the hazard risks and evaluates existing mitigation efforts. The Hazard Assessment should address the location and boundaries of the hazard, the potential magnitude of an event, and the likelihood of each event.

Many building fire codes represent minimum standards. Consider additional measures to reduce overall risk.
relationships (e.g., response time, access and, familiarity with the facility).

**Hospital security and alarm assessment**
The hospital security and alarm assessment evaluates the adequacy of both security and equipment alarming, facility accessibility, security breach rates, alarm center routing, and alarm response procedure issues.

**Environment assessment**
The environment assessment evaluates settled and airborne contamination, air filtration, environmental impact on equipment, occupant comfort level and overall facility cleanliness, as well as the outdoor air source and ventilation rate, and the vulnerability of support systems such as the HVAC (Heating, Ventilating and Air-Conditioning).

**Power assessment**
A power assessment determines the adequacy of back-up power systems, surge suppression, primary power source reliability, power routing diversity, connector systems and other energy reliability factors.

Once the plan has been developed, it must be subjected to rigorous testing. The testing process itself must be properly planned and should be carried out in an environment that realistically simulates authentic conditions, by the actual individuals who will undertake those activities in the event of emergency. Testing disaster recovery plans, alarms and procedures, conducting building inspections and reviewing building incident reports are some sources of effectiveness measurements.

**Integration of remote facilities**
Many large healthcare networks now have dozens or even hundreds of remote facilities sprinkled around a country or region. These facilities house diagnostic centers, surgery centers and freestanding emergency rooms. This rapid growth rarely involves new buildings; instead, providers rely on acquisitions, mergers, and the purchase or lease of existing structures. Retail healthcare delivery makes sense in terms of both finances and patient care, but the widespread use of legacy buildings creates two costly energy-related problems.

First, providers inherit whatever temperature controls come with the building, which are usually simple thermostats. Without intelligent controls, money is wasted on lighting, heating, cooling, ventilation, and other
building systems. Second, without effective building controls, there is no way to ensure that patients and staff have a proper, comfortable, and productive environment.

This shift to remote facilities can sometimes present issues to operational support staff. They need to maintain these sites but do not have the resources to send staff on site to the location. As a result, remote monitoring of the infrastructure begins to play a major role.

These sites must also be integrated into any business continuity/disaster recovery planning. There will be no one-size-fits-all for the various remote facilities. Factors such as facility size, age, and type, geographic locations and the nature of processes to protect will all be different. One common thread, however, will be the need for a business continuity plan. Multiple facilities in various locations, however, does offer some measure of protection, if sites can act as a partial backup for other sites should a disaster occur.
Enhancing System Availability

A recent industry trend, the concept of an “intelligent” hospital infrastructure, addresses the heart of the business continuity issue. The mechanism that enables an intelligent hospital infrastructure is an integrated control platform that maintains a complete archive of all system events, consolidated into a single reporting structure for effortless search and retrieval.

**Intelligent hospital infrastructure**
The intelligent hospital infrastructure provides maximum system uptime through a resilient design that incorporates sophisticated power distribution, management & monitoring techniques. The result is a level of system availability that is higher than what was possible via conventional, separate discrete systems.

The design of the infrastructure facilitates a distributed intelligence. This implies that systems interoperate in different ways across multiple departments of the facility. The architecture will allow for operational gains such as reductions in energy consumption through active monitoring of energy resources, improvement of patient and staff safety through intelligent access control systems, and improved environmental control (lighting, temperature, humidity) in patient rooms. The infrastructure is designed to allow interoperability of all services across the healthcare facility.

The infrastructure is also built to easily adapt to expansion and change. Using open protocol technologies, the infrastructure integrates new technologies or a new wing to the facility in a rapid and cost effective manner. The World Health Organization (WHO) estimates that in the United States alone, $335 billion a year is wasted in healthcare due to the lack of interoperability of information systems. The efficiencies gained from an intelligent hospital infrastructure helps to reduce that waste.

The World Health Organization (WHO) estimates that in the United States alone, $335 billion a year is wasted in healthcare due to the lack of interoperability of information systems.

---

A business continuity-oriented intelligent hospital infrastructure is designed to achieve the following benefits:

- High speeds of data entry and retrieval
- 7 x 24 uptime
- Secured, wired and wireless communications that integrate data, voice and video
- High reliability electrical power, HVAC, IT, and physical security equipment and architectures
- Modular, scalable systems that allow for “pay as you grow” investment without high up-front investment.
- Real-time location system (RTLS) capabilities to accelerate rapid location management across hundreds of thousands of devices

The intelligent architecture allows all systems to interoperate and for users within different departments to access the information they need to better serve their patients.

**Integrated buildings and operations systems**

If armed with the right tools, healthcare engineers, technicians, and facilities personnel are capable within their sphere of influence of producing significant hospital operational efficiency gains. Architectural and engineering design services play a key role in achieving improved health outcomes. Engineers and technicians are the ones who understand the steps that need to be taken to create an overall system design model that integrates separate sub-systems into a single intelligent hospital infrastructure.

From a healthcare facilities perspective, an intelligent technology infrastructure acts as a central nervous system for the hospital and integrates disparate systems such as power, building management, security, and IT. This enables faster and more accurate communication, as well as real-time monitoring, optimization, and automation.

What happens with such a system when the power goes out or a disaster occurs? Building Management Systems (BMS) are often the glue that holds the various operational elements of the building plant together. If the data center that supports the BMS system is protected with UPS or UPS/generator combination during an outage, the BMS system can quickly identify which parts of the hospital are still running and which are experiencing water, electrical or HVAC problems. The data from the BMS can be used as a basis for making a decision as to which systems should be restored first and what the priorities should be for recovery. Such data will help to facilitate the process of isolating critical operations from those that are non-critical. Isolated systems can then act as redundant systems if sized to handle the additional loads and arranged so they can switch from one power source to another.

**Chapters 5-6 Takeaway:** Business continuity implies a convergence of technologies and is strongly linked to intelligent power systems that are designed to be resilient.
Technology Support of Critical Applications

Physical infrastructure systems play an important role in supporting the key critical application areas within the healthcare facility. This includes support for the proper function and comfort of operating rooms and intensive care unit environments. These systems are also responsible for bringing light and power to biomedical and cardiac laboratories as well as to imaging equipment labs.

Within a healthcare facility, “physical infrastructure” typically includes the following categories of technologies:

- Power systems including such equipment as uninterruptible power supplies (UPSs), power distribution units (PDUs), circuit breakers, automatic transfer switches, isolation transformers, and generators to provide uninterrupted, conditioned, clean power to the critical loads
- Precision cooling systems that provide the optimal environment by regulating temperature and humidity
- Racks that house the critical network equipment like servers, switches, routers, and gateways
- Physical security and fire protection systems
- Cabling to interconnect equipment
- Software to monitor and manage these systems, locally as well as remotely to ensure their satisfactory operation 7x24x365
- Services to design, deliver, install, commission, operate and maintain these systems

Uninterruptible power supplies (UPS) are vital to protecting the computers that house and process patient information.

Nurse calling stations are kept running despite power anomalies when uninterruptible power supplies (UPS) are protecting the computers that house and process the patient information, for example. High precision cooling systems that preserve blood supplies need to be kept up and running and be capable of remote monitoring. Data centers and wiring closets that maintain patient records, archiving and imaging files need appropriate back up should the power supply falter.

Healthcare facility physical infrastructure is key to supporting core functionality and enabling patient care.
The sections below describe how these physical infrastructure systems support the key critical application areas within a modern healthcare setting.

**Power systems**
The hospital power system is a large complex electrical system consisting of high voltage transformers, automatic transfer switches (ATS), generators, isolation transformers, switchgear/circuit breakers, and power distribution units (PDU). The power system feeds a variety of electrical loads including lighting, heating, ventilation air-conditioning (HVAC) systems, elevators, escalators, large pumps, fans, motors, hospital security systems, medical equipment and more. The random nature of these loads (turning on and off at any time) creates an unstable power environment (i.e. sags and surges) that more sensitive imaging and diagnostic equipment and other IT networks that support them, must endure. Healthcare organizations and hospitals faced with these challenges engage engineering experts to perform complete physical infrastructure assessments that identify weaknesses and suggest corrective actions.

**Modalities**
Within a hospital context, modalities refer to high-tech medical imaging systems including Computed Tomography (CT), Magnetic Resonance Imaging (MRI), Positron Emission Tomography (PET), Ultrasound (US), and Electro-Cardiogram (ECG). These systems need to be protected from power anomalies that cause hardware failures such as blown power supplies or printed circuit boards (PCBs) as well as from system software crashes. Physical space is a major constraint for large modalities like CTs and MRIs, more so in big hospitals in urban areas, as they have no room to expand. These modalities consume a lot of power, so heat dissipation is a major challenge to the building cooling system. Often times, comfort cooling is not sufficient and precision cooling is required. One of the most critical requirements is to provide grounding isolation systems to protect the patient and the technicians from any shock hazards.

Since the hospital power grid is electrically “noisy and dirty” with sags and swells, surges and dips, it is a good practice to provide UPS protection to all sensitive, expensive electronics systems, LCD displays, workstations, printers, and peripherals. The UPS system protects the hardware, avoids unwarranted system crashes while tests are in progress, prevents loss of patient data files, and provides safe, reliable radiology examinations.
Picture archiving and communication systems (PACS)

These systems represent a broad range of technologies that enable digital radiology and digital hospitals to perform tele-radiology, tele-medicine, and tele-surgery. PACS have become more complex, encompassing systems that digitally acquire, convert, interpret, transmit, and store medical images. Diagnostic images will be available anytime, anywhere with little or no human intervention, making their distribution faster, easier, and more reliable.

PACS need to be available on demand to the nurse, physician, clinician, or specialist surgeon, providing latest imaging data of the patient under treatment. It needs to be highly available, 7x24x365 and there is little tolerance to downtime. Since the redundant array of independent disks (RAID) drives and server clusters are confined to rack enclosures, handling their heat dissipation within the racks often becomes a bigger challenge.

Hospital Information Systems (HIS) and sub-systems

Hospital Information Systems (HIS) and related sub-systems, such as Radiology Information Systems (RIS), Laboratory Information Systems (LIS) and patient health records are server-based systems running special software that make it possible to store, monitor, manage, and distribute patient medical information. They help patients in scheduling appointments, registration, and billing, and help hospitals in generating, maintaining, and managing a patient’s electronic medical records as well as generate workflow, worklist, management reporting, and a variety of other tasks. These are integrated/networked with PACS as well as various other modalities within the hospitals providing complete automation. By converting them into “digital hospitals”, they can significantly improve patient-care, minimizing human errors, saving lives, and reducing costs.

Servers and systems requiring the highest levels of availability should be identified and grouped so that they can be provided with longer runtime and higher levels of redundancy in a separate area, and in separate racks within the data center. This concept of “targeted availability” helps increase availability of business critical systems without having to incur a large capital expense for the entire data center. Higher levels of redundancy like dual feeds with dual generators and dual N+1 UPS with dual power paths all the way to the rack should be considered for highly-critical data centers and networks.

This concept of “targeted availability” helps increase availability of business critical systems without having to incur a large capital expense for the entire data center.

Physical security systems

In the realm of physical security, hospitals have a growing need for security solutions to protect patients and staff. According to a 2012 study by the Joint Commission (US-based healthcare certification body), the number of reported
homicides, assaults, and rapes in US healthcare facilities increased almost 300% over a recent five-year period.\(^6\)

In addition to patient and employee safety, failing to implement the necessary physical infrastructure can result in unexpected downtime, and safety compliance issues, which translates into lost revenue and exposure to expensive litigations, negatively affecting the bottom line.

Physical security addresses the use of security hardware, including access control, Closed Circuit Television (CCTV), door locks, monitoring systems, emergency call boxes and intrusion alarms. Below are examples of key physical hospital security systems:

- **Access control systems** – Access control systems regulate who is able to enter a building through devices such as electronic card readers and electronic locks on doors.
- **Intrusion detectors** – Intrusion detectors use sensors to detect either the open or closed status of protected points of entry. They can also determine the presence of a person in an area and the place where the alarm terminates.
- **Surveillance systems** – Surveillance systems use video cameras and monitors to alert people to events. Surveillance equipment is generally comprised of television cameras and monitors, video amplifiers, video switches, video recorders, audio recorders, and related cables, fittings and attachments.
- **Traffic control** – Vehicle traffic and parking should be controlled to prevent unauthorized vehicles from entering the property. The use of fences, gates, concrete barriers and bollards can be used to prevent and control access.

\(^6\) Joint Commission, “Sentinel Event Alert: Preventing violence in the health care setting”, June 2010

**Wiring closets or intermediate distribution frame (IDF)**

Medical imaging and diagnostic equipment are typically connected to a network. Modalities like CTs and MRIs get connected to PACS which are connected to RIS and HIS which in turn are connected to the hospital intranets and extranets. The wiring closets or IDFs, play a very vital role in ensuring the connectivity of this equipment and the availability of the network, 7x24x365. Wiring closets are comprised of layer 2 and layer 3 access and distribution switches, hubs, routers, patch panels, UPS systems with a battery back-up as well as any other miscellaneous telecommunications equipment mounted generally in a two post rack. IDFs or wiring closets may also supply power
Technology Support of Critical Applications (cont.)

over Ethernet (PoE) to networked devices like IP phones, and web/security cameras for example.

All equipment in the IDF should be protected by a UPS system. The selection of UPS should be based on:

• The total power required in watts
• The run time required in minutes
• The level of redundancy or fault tolerance desired
• The voltages and receptacles required

The UPS system is sized by taking the sum of the watt ratings of the loads. A common rackmount UPS will provide approximately four nines (99.99%) of power availability, while an N+1 redundant, UPS with built-in bypass with one-hour runtime will provide approximately five nines (99.999%), which may be sufficient for most applications. UPS products are available with battery packs to provide different durations of run time.

The plugs and receptacles required for all the equipment including the UPS in the wiring closet need to be identified. Ideally all of the equipment should be plugged directly into the back of the UPS or the transformer, and the use of additional outlet strips or rack PDUs should be avoided. However, if there are many devices, it may not be practical and a rack PDU should be used. In that case a high-grade rack PDU specifically designed for the purpose should be used. The PDU should have enough receptacles to plug all the current equipment with some spares for future needs. PDUs with a meter displaying the current power consumption are preferred as they reduce human error like accidental overloading and resultant load drops.

To ensure continuous operations of the equipment in the wiring closet, 7x24x365, cooling and airflow issues must be identified and addressed. The problem of heat dissipation and need for supplemental air-conditioning is most pronounced in the wiring closets which have no vents. Power dissipation in the wiring closet should be calculated to decide on a cost effective way to solve the problem.
Precision Control of Comfort and Environment

A Building Management System (BMS) provides facility managers with centralized control and promotes a facility-wide approach to managing energy and occupant comfort. A BMS can also help executive decision makers. Access to real-time data across systems greatly reduces the time it takes to diagnose and fix issues. It also provides new insights into how building systems work together, identifying opportunities to improve and optimizing overall operations. Integration makes it much easier to observe cross-system trends that indicate best practices or areas for improvement – something that is difficult to execute if all systems are managed on an individual basis.

In recent years, the power of the BMS has been enhanced through the development of new generation room controllers. By capitalizing on greater miniaturization and newer technologies like wireless networking, manufacturers have developed room controllers that integrate sensors, programming, and wiring into a single device. These devices are pre-engineered with more complete capabilities for specific applications such as heating and cooling, occupancy sensing, and lighting, as well as HVAC equipment like roof top units (RTUs) and fan coils. An electrician can easily install these application-specific integrated controllers without needing to program and wire each one individually, or test the connections. It can be as simple as installing a thermostat.

Room controllers, especially when linked to a Building Management System (BMS), can improve occupant comfort and performance in a number of ways.

**Room comfort**

Occupancy sensors use infrared, ultrasonic, or microwave technology to detect motion in a room, and then adjust the heating or air conditioning accordingly. Occupancy sensors override the standard settings of the room controller, based on actual room usage allowing for dynamic space control. Thus, if a hospital room is unused for the day, the occupancy sensor will detect this and, after a certain length of time, revert to the appropriate, lower, set point. In the case of remote facilities, room parameters can be adjusted remotely to meet special requirements. Alarms can also be sent out if a room’s temperature is out of threshold.

![Image of a patient in a hospital room with a monitor and a nurse.]({})

With newer technologies, room controllers now integrate sensors, programming, and wiring into a single device.

---

**Benefits of Building Management System (BMS)**

| Provide data on temperature history, people, locations | Track business performance data | Display energy consumption, alarms, and trend comparisons | Implement future energy-saving measures and justify investments | Validate performance and verify savings |

---

**Introduction**

How New Technologies Impact Business Processes

Exceeding Regulatory Compliance Requirements

Power, Operations and Emergency Response Coordination

Business Continuity Improvement Considerations

Enhancing System Availability

Technology Support of Critical Applications

Precision Control of Comfort and Environment

Sustainability and Energy Savings

Securing Buy-in from Executives

Additional Resources
Door/window sensors
Some room controllers offer the ability to link to sensors that can detect when doors and windows are open, and then take appropriate action—such as sending an alert to the BMS, and/or turning the HVAC system off automatically. Also, these sensors can add security value to a building and they can be linked to video and access control systems for additional hospital security benefits.

Lighting control
Room controllers can be equipped to control lighting. This is accomplished through simple wiring connections that any certified electrician can install. With this capability, patient room lighting can be scheduled in the same way as temperature controls. Like HVAC, lighting can be controlled dynamically by an occupancy sensor so that lights are turned on and off based on actual use.

CO₂ ventilation control
Room controllers can include CO₂ sensors (a requirement in many multi-purpose rooms and for newer building codes) with the ability to control ventilation fans. This allows for accurate control of the amount of fresh outside air that needs to be brought into the building, ensuring that CO₂ levels are within limits. Bringing in both tempered outside fresh air and recycled, tempered indoor air can help. The fresh air improves indoor air quality while reducing energy costs and fan wear by running the fans only when required and only introducing the correct amount of outside air.

Wireless Communications
Many room controllers are now available with wireless communications, which makes them easy and non-disruptive to install in existing buildings. This ease of installation can help cost-justify the retrofitting of most existing healthcare facilities. Wireless communication also offers significant benefits when it comes to space-planning and future reconfiguration. As space utilization needs change, there is often a need to redesign facility interiors. Wireless room controllers are very well suited for this as there is no need for expensive rewiring of communication cables.

Source: Schneider Electric White Paper “The ROI of building automation in retail healthcare facilities”
Sustainability and Energy Savings

Hospitals are large consumers of energy, and the trends have been towards both higher usage and costs. Energy use in the healthcare market has increased by 36% since 1995 due to changes in technology and data center requirements, as well as an increase in patients. Meanwhile, energy costs have increased by approximately 20% in the same time period. In regions where a high percentage of hospitals are in older buildings, energy efficiency is low. On average, 75% of a hospital’s energy usage stems from lighting, heating, cooling and ventilation, and hot water heating.

Remote facilities often operate at full energy use even when the offices are closed, with equipment, temperature settings, and lights operating around the clock. Any gains achieved by installing energy-efficient lighting (a common and easy upgrade), have been offset by energy-consuming technology such as electronic imaging equipment and fully digital recordkeeping. A typical clinic or other remote facility can be losing up to USD 27,000 annually per building on energy use. For a network with hundreds of locations, the loss can be in the millions.

---

Sustainability and Energy Savings (cont.)

Energy management system
Today many healthcare organizations lack sufficient processes to capture energy-consumption data and monitor performance. This hampers their ability to measure where they stand today and how successfully any efficiency initiatives would improve performance in the future. When decision-makers and investors are unable to quantify estimated savings expected from implementing energy-efficiency measures, they are less willing to fund such investments.

The inability to quantify improvements in efficiency may also prevent healthcare organizations from taking advantage of energy-efficiency incentives offered through legislation. Even in organizations where energy data is getting captured, it may not always be accessible to decision-makers.

Often the tools to analyze the data are not in place, making it difficult to translate data into actionable intelligence and practical, cost-effective recommendations. Establishing an energy data monitoring process starts with the design of the sub-metering site plan/structure. Sub-metering energy data enables process-specific energy diagnostics, which is a key tool in identifying energy-intensive processes on site, uncovering sources of energy waste, and therefore effectively prioritizing measures that will have the greatest impact on improving energy efficiency.

Modern energy management systems can now monitor the power reliability of each component and critical circuits across multiple facilities. Operators are provided with the information they need to extract the highest possible reliability from the power consuming assets as a whole. The performance of the power system as well as the performance of individual components can be benchmarked against design specifications and industry standards. Microprocessor-based devices embedded within an energy management system are permanently installed at key power distribution points, or on critical equipment, turning electrical and other physical measurements into digital data. Multi-port, multiprotocol communications allow each device to share simultaneous information with a variety of systems and users.

These new technologies now allow healthcare facility staff quick and easy access to screens that enable them to control and monitor energy consumption in patient rooms that are either occupied, or not occupied. From an energy and comfort perspective, these rooms need to be managed differently. Sensors within the rooms gather an abundance of comfort, safety, and energy consumption data and building analytics software converts that data into actionable intelligence that improves the energy efficiency performance of the facility and boosts patient satisfaction. The artificial intelligence built into the system identifies...
Sustainability and Energy Savings (cont.)

problem conditions in the various rooms and then offers suggested proposals and actions to address the situation. This type of automated fault detection and diagnostics is sent to cloud-based data storage. The data in the cloud is analyzed by qualified experts. The reports generated from this data, in addition to identifying equipment and system faults, identify a prioritized sequence of operational improvements, and energy usage trends. In addition, avoidable costs, total energy savings during pre-defined periods, and analyst commentary are provided.

Other energy savings best practices
These types of energy management services can supplement the way building management systems can boost energy efficiency for a facility. Other energy saving best practices that integrate with the BMS include:

• Variable speed drives integrated into physical plant pumps and motors
• Power metering for accurate measurement and reporting of consumption
• Load management so that electric utility bills can be managed to reduce expense
• Retro-commissioning and audits so that potential downtime problems are identified before they occur
• Greenhouse gas monitoring so that the healthcare institution can play its part in reducing global warming

Chapters 7-9 Takeaway: Modern technologies are focused on greater control of facility performance and simplification of the management of the healthcare facility ecosystem.
Securing Buy-in from Executives

The reputation of the healthcare organization and the overall quality of patient care are the drivers that enable growth and prosperity. Growth is fueled by innovation, and that includes both business process innovation and technology innovation. Therefore, facilities and operations personnel have an important role to play in terms of supporting the goals of the executive leadership through the introduction of innovation. A key challenge facing operations and facilities personnel is how to achieve buy-in from executives for the funding of technology upgrade projects. The critical success factor is the ability of facilities and operations personnel to communicate the functions of new technologies into terms that reflect business value.

Executive priorities
Hospitals directors and administrators are concerned with several main business issues:

• **Maintaining financial stability through the generation of healthy revenue streams and profit margins** - This implies a consistent high volume of patient flow, growth in sales of additional services, reduced cost through higher hospital staff efficiency, reduced energy consumption, and the avoidance of liability situations.

• **Maintaining patient safety by embracing the “first do no harm” mantra throughout the organization** - This translates into facility and systems reliability and quality, so that patients are protected from any unforeseen accidents during their stay in the hospital.

• **Maintaining patient satisfaction** - This ensures a positive public image and a reputation for quality service which enhances future revenue streams.

• **Increasing levels of hospital security** - Both physical and data security have become higher priority investments.

Improved hospital operational efficiency and connectivity have to translate into a language that reflects cost reduction, faster turnover, and higher return on investment. Healthcare executives often express frustration that subordinates lose them in detailed discussions surrounding watts per square foot, human machine interfaces, and protocol convergence. Oftentimes those discussions end with facilities and IT teams failing to acquire the funding they need to move technology innovation forward.

The language problem is compounded by the fact that the benefits of innovation are often invisible or gradual. “Smart” monitoring systems that manage the performance of a hospital, for example, are unseen by most of the organization’s employees. Yet this “behind the wall” innovation builds profit through hospital operational efficiency and connectivity-inspired business productivity gains.
Securing Buy-in from Executives (cont.)

Improved hospital operational efficiency and connectivity have to translate into a language that reflects cost reduction, faster turnover, and higher return on investment.

When selling innovation to hospital executives facilities and IT personnel need to emphasize these three points:

1. Highlight the practical business benefits of the technology or process improvement being proposed.
2. Explain the side benefits of how innovations that improve hospital operational efficiency also drive sustainability thereby enhancing competitive advantage and boosting public image.
3. Emphasize that deploying innovation is not a one-time, one project benefit and discuss future improvement potential.

Facilities management selling strategies

Regarding facility infrastructure, healthcare facility executives focus on three main points: reliability, traceability, and liability. They want to ensure that hospital systems are as reliable as possible, to reduce any failures in the emergency system. Through the use of accurate tracking tools, they want to ensure traceability so that, should an unanticipated incident occur, proof can be provided that the healthcare facility acted according to safe, legal and ethical practices. They also want to ensure they can show the events that led up to any failure in case of litigation, and to protect the hospital from liability. They have to rely on the facility manager to ensure the system is reliable and that appropriate reports are being created, but generally don’t have much insight into what is being done or whether it is sufficient. This is where facilities and IT teams can provide the guidance.

Effective IT systems are crucial to meeting all of these objectives, whether it’s the move to electronic health records, digital radiology or telemetry systems that show patient vital stats on large in-room screens. IT is becoming increasingly mobile, with “computers on wheels” increasingly giving way to mobile devices used at the patient bedside and used for recording data, and checking for drug interactions.

Healthcare facility executives focus on three main points: reliability, traceability, and liability.
Facility and IT teams need to also communicate to their executives the cost of inaction when outdated technologies are not replaced or upgraded. Estimated cost of downtime for healthcare facilities, for example, is approximately $636,000 an hour on average (does not take into account the impact of potential deaths caused by emergency power supply failures). Healthcare facilities have experienced hundreds of millions of dollars in lost revenue from cancelled services, legal liability, and damaged reputations as a result of unanticipated downtime.

To avoid these worst case scenarios, facility teams need to build proposals that reflect an investment prioritization roadmap that allows executive to make the right technology decisions. Technology proposals should include the following touchpoints:

- **Investment returns**
- **Demonstrated reduced risk**
- **Resources required**
- **Metrics to be deployed to show return**
- **Roles and responsibilities of those involved**

Technology innovation will improve ROI in several ways. Access to real-time data across systems reduces the time it takes to diagnose and fix issues, provides new insights into how building systems work together, and creates opportunities to improve and optimize overall operations. Integration across buildings makes it easier to compare facilities and identify best practices or areas needing improvement – something that is difficult to do if all systems are managed individually.

Regions with wide temperature fluctuations will usually see large savings in heating and/or cooling costs. Buildings with a strong southern light exposure can adjust HVAC and lighting based on actual conditions rather than on a fixed schedule, taking advantage of natural heat and light to reduce energy use. While specifics vary, every building should be able to benefit from improved energy control and management.

The estimated cost of downtime for healthcare facilities is approximately $636,000 an hour on average.

Just upgrading to stand-alone intelligent controllers can reduce lighting expenses by as much as 40%, and cut overall energy costs by 20% or more. With full Building Management System (BMS) implementations, savings of 30% and more are not uncommon.

By integrating power distribution with building and hospital security systems, healthcare facilities can realize savings that can help improve financial performance while protecting and better serving patients.

Designing or retrofitting integrated solutions for healthcare facilities – connecting power distribution, building management, IT, and hospital security – can aid healthcare enterprises in achieving their objectives for superior patient care and satisfaction, a safe environment for patients and staff, positive financial performance, and long-term productivity.

---

Technology is now core to the delivery of quality healthcare.

Conclusion
Patients interact with technology almost from the moment they step into a hospital. From registration to the point where they’re outfitted with bar-coded ID bands, to IV pumps, computerized physician order entry systems, and lots more. Technology is now core to the delivery of quality healthcare.

As a result, hospitals also have a requirement for continuous, uninterrupted power to ensure the whole facility infrastructure and these distributed IT systems are always on. This is where the need for coordination between facilities and IT organizations comes into play. Without proper coordination, healthcare facilities run the risk of violating various building and healthcare regulations.

The hospital’s physical environment clearly has a huge impact on the health of patients. Unfortunately, hospitals are causing harm to patients and wasting money on avoidable events. Preventable adverse patient events account for 440,000 deaths—roughly one-sixth of all deaths that occur in the United States each year.10 These figures are conservative. Other research shows that hospital reporting and peer-review systems document only a fraction of patient harm or negligent care.

Many of the individual behaviors preceding these dangerous events or errors are undetected by the human eye and therefore are unforeseeable. However, this situation can be corrected. Patient hazards within hospitals can be made visible with intelligent and automated building solutions that bridge the disconnect between the structure and function of a hospital. As a result, the transmission of healthcare-associated infections, patient falls, medical errors, and wrong site surgeries can be greatly reduced.

By modeling a hospital’s infrastructure to enable safe behavior, hospitals can greatly improve clinical outcomes, shorten inpatient stays, decrease readmissions, and reduce hospital expenditures.

Chapter 10 Takeaway: Any proposals presented to executives surrounding expenditures on infrastructure technologies will need to be tied to business value.

---

## Additional Resources

### White Papers

- **Power Protection for Digital Medical Imaging and Diagnostic Equipment**
- **How Secure Power Solutions Support Healthcare Facility Infrastructure Stability and Safety**
- **Automating Emergency Power Supply System Testing in Hospitals**
- **Assessing the Health of Your Healthcare Facility’s Electrical Power Distribution System**

### Blogs

- **How Can You Leverage Manufacturing Quality Improvement Techniques to Improve the Reliability of Your Healthcare Facility**
- **3 Core Challenges of Installing and Supporting Sophisticated Diagnostic Equipment in Hospitals**
- **Secure Power in Healthcare: Taking Care of the Pain Points**
- **The Internet of Things Demands New Thinking about Power Protection for Mains and Brains**
- **Secure power for healthcare spans range of solutions**
- **Explosion of Technology in Healthcare Requires Cooperation Between IT and Facilities**
- **GridEx II Serves as Reminder on Grid Reliability and Secure Power Preparedness**