Preparing Your Hospital for a Crisis

An IMEG Executive Guide

THE IMPORTANCE OF HEALTHCARE RESILIENCY

When disaster strikes, hospitals and healthcare systems are on the front line of ensuring community safety and resiliency. However, this purpose can only be served if your hospital is prepared to face the worst. By taking proactive steps and making concrete plans to further the disaster preparedness of your healthcare facility, you'll be better equipped to answer the call of your community during dire situations.

Establishing a disaster-resilient healthcare institution has become exceedingly more complex—and continues to evolve. The COVID-19 pandemic revealed the extreme need for resiliency to infectious outbreaks. Today's healthcare institutions also need to be resilient in the face of power outages, water shortages, and infrastructure failures—not to mention active shooter events, mass casualty events, and cyberattacks that can lead to financial loss or breach in patient privacy. The changing climate also has increased the frequency and severity of natural disasters such as wildfires, tornadoes, hurricanes, and flooding.

Given such a broad range of potential threats, healthcare organizations must ensure their hospitals are adequately prepared to be able to continue providing lifesaving care when a threat becomes a reality.

Even hospitals that feel confident in the resiliency of their building may find gaps and inconsistencies in their contingency plans—e.g., the ability to handle patient surges and patient acuity in response to a pandemic.

This executive guide provides a high-level overview of the major considerations that can help organizations begin to chart their path toward true and comprehensive healthcare resiliency.

IMEG
The FUTURE. Built Smarter.

Characteristics of resiliency

Achieving resiliency first requires an understanding of four commonly accepted characteristics of infrastructure resiliency, as defined by the National Infrastructure Advisory Council:

- **Robustness—the ability to maintain critical operations and functions in the face of crisis.** For healthcare, this includes the building itself, the design of the infrastructure, and system redundancy or substitution.
- **Resourcefulness—the ability to skillfully prepare for, respond to, and manage a crisis or disruption as it unfolds.** This includes identifying courses of action and continuity planning, training, supply chain management, prioritizing actions to control and mitigate damage, and effectively communicating decisions.
- **Rapid recovery—the ability to return to or reconstitute normal operations as quickly and efficiently as possible after a disruption.** Components of rapid recovery include carefully drafted contingency plans, competent emergency operations, and the means to get the right people and resources to the right place.
- **Redundancy—having back-up resources to support the originals in case of failure.**

Using these traits as a benchmark, you can begin to take an informed look at the main resiliency issues facing your healthcare facility. You can then conduct a thorough vulnerability assessment to discover ways your building and operations may fall short. The vulnerability assessment can be broad or threat-specific, but it is critical to be thorough and include key team members within the health system and third-party experts as required.

5 key areas of multidisciplinary healthcare resiliency

According to the National Institute of Building Sciences, “Resilience is multidisciplinary and needs the cooperation of different disciplines for successful outcome. Without multidisciplinary cooperation and contributions, there cannot be successful or efficient resilient infrastructure.”

For healthcare, multidisciplinary resilience must involve five key areas to ensure your institution is ready to survive a crisis, each of which is broadly examined in the following chapters.

Chapter 1: Natural Disasters and the Structural Integrity of Your Hospital
Chapter 2: The Effect of Disaster on Your Hospital’s MEP Infrastructure
Chapter 3: Hospital Physical Security—Beyond Guards and Cameras
Chapter 4: Reacting to Mass Casualty Events and Infection Outbreaks
Chapter 5: Protecting Your Hospital from Cyber Security Vulnerabilities

These key areas represent many of the overlooked and misunderstood aspects of hospital risk management. Each area also is complex and will require detailed expertise to achieve true resiliency. By using this guide as a starting point for thoroughly examining each area within your institution, you can start the journey toward ensuring your hospital is better prepared to handle a crisis.

This fallen stair tower at a hospital was the result of the San Fernando Earthquake of Feb. 9, 1971. (© U.S. Geological Survey)

Chapter 1: Natural Disasters and the Structural Integrity of Your Hospital

Natural disasters may be unstoppable, but that does not mean your hospital cannot take intentional and necessary steps to lessen their impact. While the specific natural disasters you should be concerned about—and many of the specific actions you should take in response—depend on your geographic location, there is no such thing as being too prepared.

In addition to tornados, hurricanes, floods, wildfires, and earthquakes, there are other weather- and terrain-related events—derechos (land-based, straight-line windstorms), heat waves, mudslides, avalanches, and tsunamis—that are considerably less common but still can impact your operations based on their proximity. The structural and architectural design of your building does not necessarily need to take every potential natural disaster into account, but it should consider common events for your area, as well as potentially devastating chance occurrences, such as fire.

Beyond establishing procedures and educating your staff on hospital policies in the event of a natural disaster, there are several factors about your hospital structure that you need to consider.

Determine if you want your hospital to serve as a community beacon

In times of great tragedy or upheaval, communities often turn to hospitals to act as a gathering place or safe landing amid the chaos, even if they don't need medical care. Assuming your hospital makes it through whatever disaster befalls your community, you'll need to consider whether you want your hospital to be a place of refuge.

If the answer is yes, you'll also need to put in place procedures to ensure your hospital is prepared to take on this role. First and foremost is the designation of a disaster response area—ideally one that is hardened against potential disaster effects and prepared to take on an influx of people.

Identify any challenges posed by the physical design of your building

Consider how the layout of your building would function in a disaster. For instance, are your emergency generators or back-up fuel pumps in the basement? This could leave your hospital without these critical systems in the event of a power outage if your basement experiences flooding.

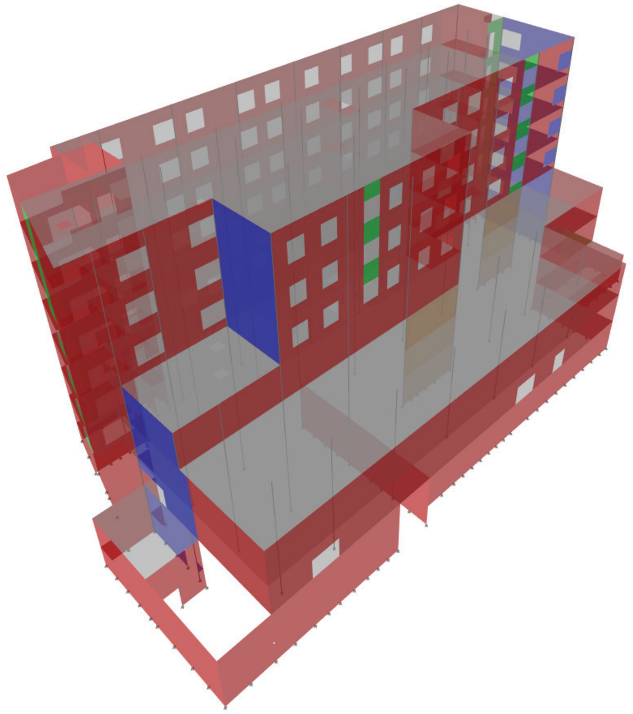
Also consider the locations of the emergency exit stairwells in your building. Ideally, they should discharge into remote areas of your hospital that aren't high risk for damage or, in the case of an active shooter, a physical attack. To create safe fire exits, stairways should also be maintained with positive pressure from a clean source of air, which will help keep smoke and toxic fumes out.

Since there are numerous variables in the physical design of your building that could become hazardous during a natural disaster, the safest and most thorough course of action is to conduct a full building vulnerabilities assessment with a professional.

Examine structural hardness in response to adverse conditions

"Hardness" refers to the process of reinforcing individual systems within your hospital to make them more resilient. For example, during a natural disaster, your building could be subjected to high winds and substantial rains. By hardening your building to take on these outside forces, you can minimize damage and ensure critical areas remain safe, allowing your hospital functions to continue.

While building codes require your building to be able to withstand a certain wind level, further hardening may be necessary if hurricanes and tornados are common in your area.



IMEG has completed several healthcare seismic retrofits in California and is working on several other building upgrades. Above is a computer-generated 3D structural analytical model of one of the upgrades.

For example, Mercy Hospital in Joplin, MO, opened a new, hardened, nine-story patient tower and five-story clinic in 2015—four years after its previous building sustained extensive damage from an EF-5 tornado. The new hospital incorporates window and wall systems that are designed for 250-mile-per-hour wind speeds around the neonatal and intensive care units to protect the most vulnerable patients; other areas of the hospital have an exterior wall system designed for higher wind speeds to provide additional resiliency. The hospital also has a standalone, hardened central utility plant located away from the main hospital with a reinforced concrete tunnel connector.

Seismic resiliency also must be addressed and is enforced by code in hospital buildings along the West Coast and particularly in California, where earthquakes are prevalent. Seismic resiliency also must be addressed in non-essential healthcare campus buildings in these areas. (See "Seismic considerations for non-essential buildings" at right and read the IMEG executive guide, "Seismic Retrofit: A Guide to Achieving Compliance for California Healthcare Organizations.")

***Summary:** Preemptively improving the resiliency of your hospital through architectural and structural changes and infrastructure support can make all the difference in your facility's ability to withstand a natural disaster.*

Seismic considerations for non-essential buildings on healthcare campuses

New, non-essential healthcare campus facilities such as medical office buildings, clinics, and parking ramps are not typically designed to the higher strength and detailing requirements of the hospital building and could see more damage and hindered operations following an earthquake. Therefore, critical services (sterile processing, imaging, etc.) and MEP infrastructure routing should be minimized in these facilities.

Caution also should be exercised when considering the placement of new functions, MEP infrastructure, and ingress/egress within and adjacent to existing buildings and parking ramps. These older buildings—especially those constructed in the mid-20th century—typically were not designed by today's seismic standards and unless retrofitted are at a higher risk for partial wall collapses and excessive building movement after a major earthquake.

Chapter 2: The Effect of Disaster on Your Hospital's MEP Infrastructure

Maintaining the inner workings of your hospital's vital systems is also crucial to the continuing operation of your building during a natural disaster. The mechanical, electrical, and plumbing (MEP) infrastructure of your facility needs to be sufficiently protected and hardened against potential events to remain operational. Without adequate power (see "Microgrids" on page 5), ventilation, and water, your hospital will quickly lose its ability to provide services and safety to patients and staff.

To increase the resiliency of your hospital's MEP infrastructure, first determine what level of continuity your systems will need to maintain in the event of a disaster. Next, consider the types of threats your systems may encounter and what vulnerabilities they would face against those threats. Your best course of action is to bring in an MEP engineer to thoroughly assess your facility's risks and gaps, the following key concerns and approaches should be considered.

Location, routing, and bracing of infrastructure

As stated in Chapter 1, it's common for facilities to have electrical equipment and emergency power infrastructure located in the lower level. While it might initially seem to be a good idea to have these systems in non-premium space, locating them in the lowest level of a building increases the risk of flood damage. This is especially dangerous if your hospital is in a floodplain, or if your building is at or below sea level.

During the planning stages of a new facility, one of the simplest steps you can take to reduce the risk of flooding affecting your MEP systems is to **locate critical equipment at higher levels**. For example, the generators at Memorial Medical Center in uptown New Orleans were able to withstand the initial impact of Hurricane Katrina in 2005, but the flooding over the following days reached the emergency power transfer switches, expediting the evacuation of the facility.

Routing of critical infrastructure such as emergency power, chilled water, and steam through a campus is typically supported from trestles, tunnels, and through nonessential and older buildings. The routing of these elements can sometimes be the weak link in keeping the hospital operational if the facility is hit by a severe earthquake. It is critical, therefore, that the physical infrastructure supporting these major MEP components be designed to the same high classification as the healthcare areas they serve farther down the route to ensure their performance after an event.

Another aspect to consider with the major MEP infrastructure is the **seismic bracing** and expansion (flexible) joints of trestles and tunnels from the central utility plant to the various critical points of use. Seismic bracing is required for larger and critical function components to ensure they have sufficient support, move with the building, and flex between two buildings.

Hardness of systems

In some instances, hardening of systems can be accomplished by location. During the planning stages of the Advocate Summit Hospital in Wisconsin, for example, it was decided to locate the central utility plant 500 feet away from the hospital, connected with a utility tunnel. One of the main drivers for segregating the plant from the main hospital was to hedge against a disaster potentially impacting both locations simultaneously. The remote plant also allowed for the space to house underground fuel storage to allow the generators to run for 96 hours.

By hardening their utilities in this manner, the replacement hospital building is far more prepared should disaster strike.

Redundancy

Baseline redundancy for critical infrastructure items such as boilers, medical gas, and power are required by code for healthcare facilities, but additional redundancy should be a key consideration when evaluating the resiliency of your MEP systems. For instance, assume your building load is 1,000 tons of cooling and you have two 500-ton chillers. If one chiller breaks down or is compromised, your facility will only have 50 percent of the required cooling capacity available. To safeguard against this potential problem, you could plan for one of the following:

- Purchase a back-up 500-ton chiller in case of emergencies
- Have three 500-ton chillers to have an N+1 capacity, or, in other words, 100 percent back-up available should a single chiller fail
- Upsize both of your chillers to 750 tons so you'll still have 75 percent of what you need if one fails
- Install outside piping to bring in an emergency back-up chiller when needed

Though this example is specific to water chillers, the same logic can be applied to other major infrastructure. Having a back-up boiler, for instance, ensures that critical functionality—heating for staff and patients and heated water to sterilize critical equipment—is not lost if something happens to the main boiler. Ideally, the main and back-up boilers would be connected on the same network so the back-up could immediately begin working after the main boiler fails, thus leaving no gaps in service.

The importance of having redundancies and back-up plans can be applied to all necessary systems and processes—emergency generators, air handling units, critical distribution pumps, and even your plumbing system, without which you would not be able to flush toilets.

Potable water

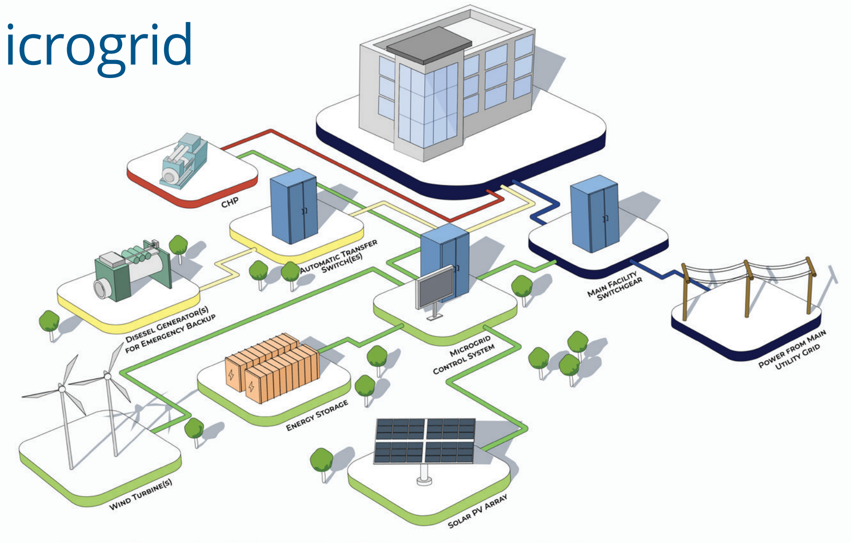
Other than pallets of bottled water, it's rare for hospitals to store water. This can lead to significant problems if something interrupts your water supply. How would you flush toilets? How would you wash and sterilize equipment? How much drinking water would you need over a fixed period of time?

To answer these questions, first determine how much water usage you truly have at your facility. A week's worth of water might not be as much as you think. Once you understand your usage, you can make an informed decision on how much water you'll need to access in an emergency. While on-site water storage is the best solution to this potential problem, you can also contract with a pumper truck to be available in emergency situations.

Beyond planning for access to water in case of emergency, you can also enact procedures to save and reuse water. Plan to shut off water to designated, non-essential areas of the hospital, use recycled water to flush toilets, or install a roof drain for condensation recovery.

Summary: *The process for making your MEP infrastructure more resilient involves careful thinking and consideration of your hospital's specific functions and needs. By addressing vulnerabilities in your systems ahead of time, you can avoid the challenges and tragedies that can occur when hospitals get caught unprepared.*

Microgrid


CHP
Automatic Transfer Switch(es)
Diesel Generator(s) for Emergency Backup
Main Facility Switchgear
Microgrid Control System
Power from Main Utility Grid
Energy Storage
Wind Turbine(s)
Solar PV Array

With the future stability of regional power grids more in doubt than ever, a microgrid is an emerging solution for hospitals and other healthcare facilities that face the critical task of establishing a long-term source for their "always on" power needs.

This freestanding power source provides not only for the resiliency of hospitals during long-term power loss, but also helps organizations meet sustainability goals, reduce their carbon footprint, and combat the rising costs of energy.

A microgrid can be made up of solar panels, wind turbines, combined heat and power plants, generators (diesel or natural gas), and battery storage—all of which produce power to serve the facility and go beyond current requirements for temporary back-up power.

Adopting microgrid technology provides future proofing against actual, plausible disaster scenarios that could result in a long-term loss of power availability. In California, for example, rolling blackouts, rising energy costs, and wildfires have made the resiliency of the grid extremely suspect. There, as well as in any location facing a significant power disaster, 96 hours of generator fuel may not be enough. Moreover, the regulatory requirement for back-up power presupposes that, should the interruption persist longer than 96 hours, replenishment fuel will be accessible—an assumption that might not hold true. In such circumstances, a microgrid could save lives.

For more information, listen to a related IMEG podcast and read the executive guide, "Microgrids for Healthcare Facilities: 'Island Mode' Ensures Independent, Long-term Operability."

CPTED strategies include the use of vegetation, bollards, and establishing clear pathways toward desired entrances to a building.

Chapter 3: Hospital Physical Security—Beyond Guards and Cameras

By their very nature, hospitals should be safe places. Yet, despite the amount of healing that occurs within the walls of a hospital, the physical security of the building is often at high risk.

Hospitals are vulnerable to physical dangers since they are open all the time and accessible to the public, providing potential intruders easy entrance. In addition, patients and visiting family members often experience stressful or traumatic experiences within the hospital, which can heighten emotions and reactions. In fact, workers in a healthcare setting are five times more likely to be victims of workplace violence than private industry workers.

Considering these factors, the physical security of your hospital is clearly an important piece of healthcare resiliency. However, safeguarding your hospital from a malicious intruder or physical attack requires more than basic security measures like guards and cameras—and it all starts with restricting and controlling access to your building.

One of the most effective ways to increase the physical security of your hospital without creating an overly institutionalized aesthetic is by leveraging architectural elements to create secure environments. These strategies are called Crime Prevention Through Environmental Design (CPTED). The following paragraphs outline how you can incorporate these principles and other security strategies into your exterior space and hospital entrance design.

Restrict access points to the building. Ideally, you want your hospital to have designated, specific entrances for public access. This allows for easier monitoring and gives you the option to set up secure visitor screening. Utilizing vegetation and various architectural elements can help drive people away from entrances you don't want them to use and toward your main entrance. While you need to have numerous egress doors to meet code, there are steps you can take to ensure your emergency exits are only used in the case of an emergency. With proper signage, alarms, camera monitoring, and even removal of exterior-side door hardware, you can better control which doors permit entry into your hospital.

Separate visitor and employee parking lots. One of the biggest physical security concerns every hospital should have is for its staff. To limit the potential for interactions with upset patients or angry family members and visitors, keep public access points separate from employee access points. By establishing a perimeter boundary for an employee parking lot, you can create a level of protection within the parking area so staff can move back and forth to their vehicles safely.

Utilize effective parking lot lighting. More than brightly lit parking lots, you need evenly lit parking lots. When lighting is too bright in some areas, it can have the effect of making other areas seem darker. Instead of using big, bright lights, utilize smaller, more numerous lights that have a high level of distribution over your parking lots. This can play a significant role in security by increasing visibility and improving camera coverage.

Create vehicular boundaries. Pedestrian traffic needs to be protected from vehicular traffic, and creating a clear separation between the two can minimize incidents. For instance, instead of just a crosswalk, consider using pavement changes, lighting changes, and rumble strips to draw attention to the separation. You can also use CPTED principles to restrict vehicle access to buildings through bollards and curbing. Just ensure the restrictive elements you're using have practical stopping power, rather than just aesthetic appeal.

Limit access to ambulance delivery areas. Separating the ambulance delivery area from the public emergency entrance will limit confusion and help ensure an intruder isn't gaining access to your hospital through a vulnerable and often chaotic area. This can be as simple as creating an environment that the public won't be drawn to or isn't readily visible from the front of your hospital, which can be done with additional vegetation or barriers.

Consider how you will handle after-hours traffic. It's common for hospitals to have all after-hours traffic enter through the emergency department. While this is a fine solution, it's still important to consider what this policy does to your parking access. How far away from that entrance are people going to have to park? What kind of exposure will they have while walking to and from their car? To make this a safe option, you may need to consider additional lighting and protective barriers.

Utilize glass vestibules as boundaries for secure entry. The entrance to your hospital should be warm and welcoming—but it also needs to be safe. Fortunately, you can increase the security by creating a glass vestibule to act as an additional set of doors necessary to gain entry. Depending on the location of your hospital and your risk for gun violence, you could consider using bulletproof glass in the entrance. At a minimum, install laminated glass so it won't immediately shatter if hit.

Make emergency departments escapable. Admitting and waiting areas in emergency departments are often high-stress spaces in which tempers can flare.

To protect your employees working in these areas, create safe points and escapable options in case they feel threatened. For instance, while a desk can act as an initial boundary, consider adding an extra layer of protection by having an additional exit behind the desk through which the employee can leave if threatened.

De-escalate by design. "De-escalation by Design" is a security concept that creates spaces that are safe, calm, and therapeutic and is particularly effective for behavioral health units and emergency departments. The goal is to defuse situations in advance so nurses and staff only resort to conflict resolution and crisis intervention as an exception, not the rule. It also creates a more aesthetic, noninstitutionalized environment that is more pleasant and less stressful to work and stay in. Ideally, the design work is done with architects in the concept and master plan phases, but it can also be done when renovating or retrofitting a space.

For more information, read the IMEG blog posts:

- "CPTED: Comprehensive Strategies to Keep People and Buildings Safe."
- "De-escalation by Design: Making Behavioral Health, ER/ED Facilities Safer"

***Summary:** While physical security at hospitals is often focused on guards and cameras, the design and accessibility of your building can be just as significant in preventing intrusion and outside dangers. By employing CPTED principles and other strategies to limit access, you can more effectively control the physical threats your hospital faces and increase your resiliency in the face of violence.*

Creating soothing spaces through a variety of design elements is part of De-escalation by Design.

Chapter 4: Mass Casualty Events and Infectious Outbreaks

When a mass casualty event strikes your community or a highly contagious infection breaks out, your hospital will need to be prepared to contain the situation and minimize the fallout. Both types of occurrences are clearly out of the normal operations of your hospital—but healthcare resiliency is all about preparing your facility to deal with the abnormal.

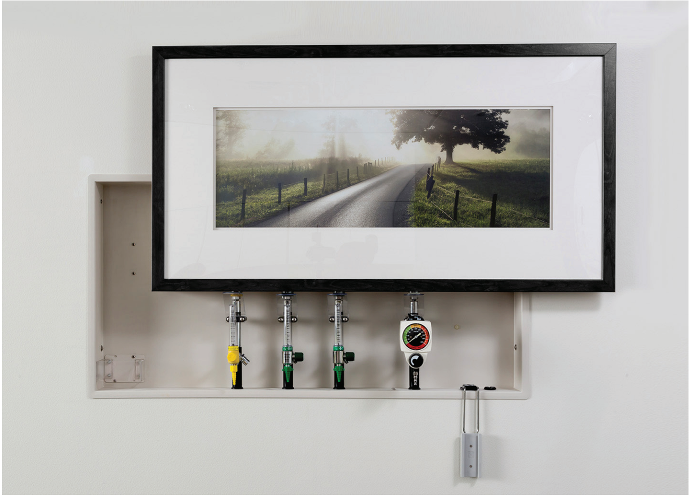
How your hospital reacts in the minutes and hours after a mass casualty event or infectious outbreak can be the difference between lives saved and lives lost. Having procedures and plans in place for quick action is essential to achieving resiliency. The specific courses of action will depend largely on your hospital's capabilities and unique situation. Such emergency preparedness is part of the much larger strategy of organizational preparedness. Here, however, are several broad questions you'll need to answer as you develop your plans.

How will you transport patients if you reach capacity? An October 2017 mass shooting in Las Vegas—the deadliest on record in the U.S.—left hundreds of victims in need of emergency surgery. Since the hospital couldn't handle every surgery on site, they had to transport patients to different facilities to get the care they needed. Consider how your hospital would react if you reached capacity and were unable to service a large, critically injured population.

Do you have the infrastructure to expand your ED quickly? Your emergency department is designed to handle a daily influx of patients—not a mass casualty event. However, you can adjust your building's infrastructure to expand your services quickly if the need arises. For instance, you can hide medical gas outlets and oxygen vacuums in a corridor to expand service locations and increase the number of patients you can treat. With specific artwork systems that can cover these outlets, you won't even know they're there until you need them.

How will you handle extra emergency response vehicles? If multiple emergency response vehicles descend on your hospital at once, you'll likely need a designated space to direct them to park. Additionally, since most hospitals only have one helipad, consider if there is a way to set up an additional temporary helipad. This can be as simple as putting pavers down in a grassy area.

Do you have a plan to manage family members and media? A mass casualty event is newsworthy and nerve-wracking. When one occurs, your hospital will likely be surrounded with media looking for the story and family members hoping their loved ones are safe. You'll need a strategy to manage this crowd and ensure they can get enough information to calm the panic.



Access to medical gas outlets can be concealed behind artwork in hospitals when not needed. (Photo © Modular Services)

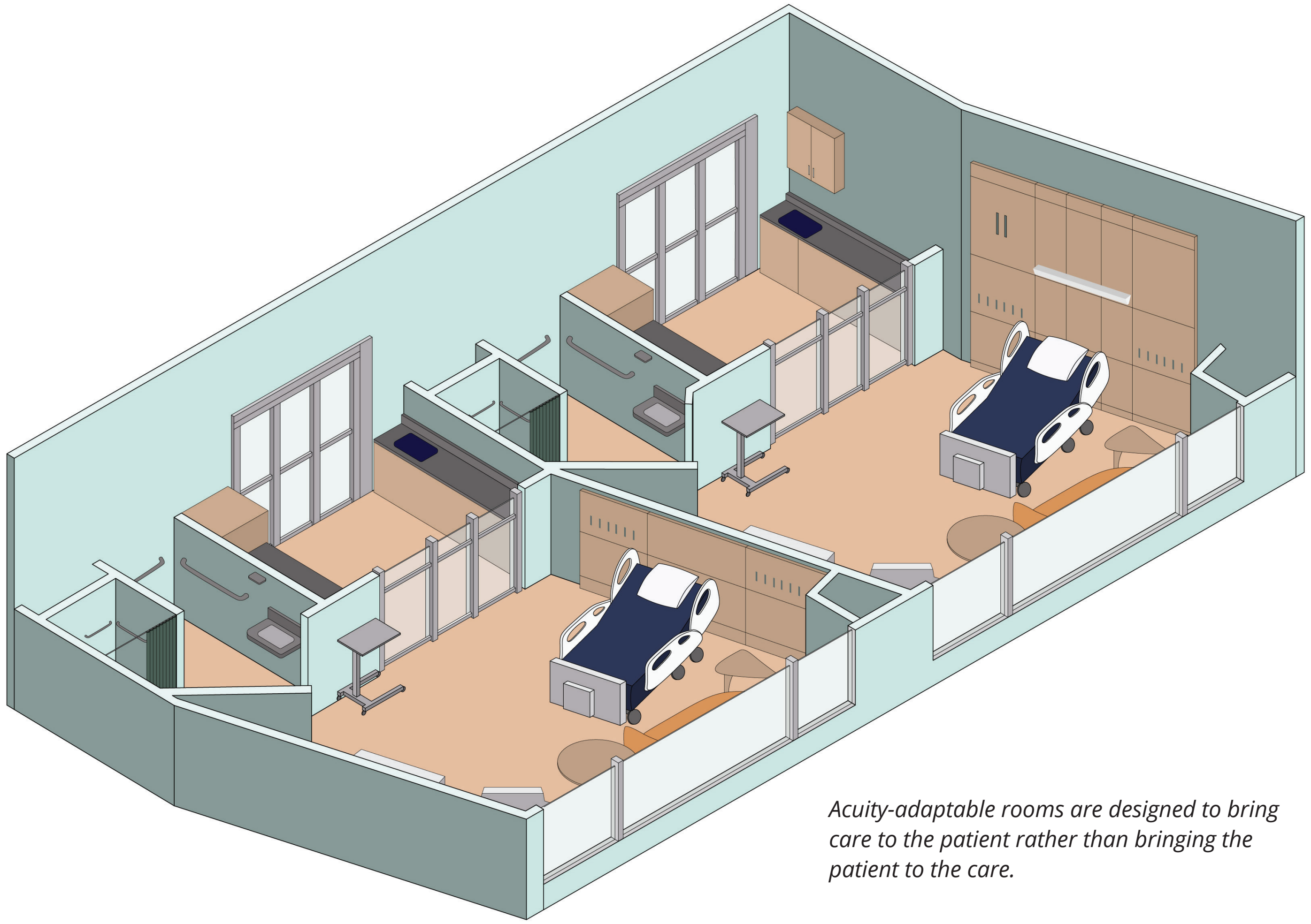
What is your protocol for quarantining a patient with an infectious disease? When you discover a patient has a highly infectious disease, you need to act quickly to ensure the least amount of exposure. That's why you need a clearly established protocol that all relevant staff are aware of and have adequate training to execute.

Do you have a permanent or temporary quarantine space? Most hospitals don't support a permanent quarantine space since it can be a substantial investment to create a space that is used rarely, if ever. For this reason, the most popular option is to have an adaptable space that can be quickly assembled when necessary. You'll need to consider where to put this adaptable space in relation to your HVAC system so you can maintain the right pressure for sterility. This type of need leads into the larger topic of acuity adaptability.

Acuity adaptability

Though it may not be the answer for every healthcare facility or system, the acuity adaptable design concept—first developed in the 1990s—could lead the way to better care in many situations involving infectious outbreaks.

Traditional models of healthcare design and delivery involve transferring the patient to different rooms, different departments, even different hospitals to be treated by different specialist physicians and nurses as the patient's condition improves or worsens. With the acuity adaptability model of healthcare design, however, the patient remains in the same room from admission to discharge, regardless of changes in acuity—potentially leading to better patient outcomes and reductions in the cost of care over the long term.



Acuity-adaptable rooms are designed to bring care to the patient rather than bringing the patient to the care.

Flexibility is the primary benefit of acuity-adaptable healthcare design, allowing facilities to adapt to the needs of the patients and communities they serve—particularly useful for inpatient rooms and "soft" spaces that could be flexed into during surge situations. Several direct and indirect ramifications of the pandemic throw the benefits of acuity adaptability into stark relief:

- Reducing cross traffic
- Compartmentalizing
- Creating distance and barriers
- Separating infectious patients

Acuity-adaptable rooms have obvious advantages in achieving these goals. By transferring patients immediately upon admittance to a single room where they will receive all care until discharge, there is little or no risk that they will infect other patients or healthcare personnel since multiple transfers from one unit to another do not occur.

To learn more, listen to the IMEG podcast episode, "Is Acuity Adaptability Feasible?" and read the executive guide, "Acuity Adaptability: Innovative Planning and Design for Responsive Healthcare Delivery."

Summary: *Mass casualty events or infection outbreaks bring multiple risks to hospitals, patients, and staff. Failing to plan for these rare but potentially deadly events could leave your hospital ill-equipped and liable, resulting in sub-par patient care. By ensuring you are as prepared as possible to address these circumstances, you can minimize their effects.*

Chapter 5: Protecting Your Hospital from Cyber-Attacks

All modern hospitals also need to be prepared for the significant threat posed by cyber-attack. Without thorough cyber security, you leave your hospital's cyber infrastructure vulnerable to a malicious breech.

It's not just external hacking attacks that you need to worry about—threats also can come from inside your network. For instance, intrusions can be introduced inside your network from an infected USB flash drive or through a vendor unknowingly creating an unprotected connection to the outside world.

The purpose of a healthcare cyber-attack is likely to be for one of two reasons: accessing electronic health records to sell on the black market or using ransomware to hijack systems and prevent access until a ransom is paid. Both types of attack can be devastating for your hospital's reputation and ability to continue to function. Unfortunately, creating a secure cyber network in today's hyper-connected world is a bigger challenge than many hospital IT departments realize.

Vulnerabilities of the IoT

The Internet of Things, or IoT, refers to all the daily devices and everyday objects we use that are now enabled with network connectivity. Objects that formerly were not connected to the network—appliances, automobiles, light switches, and televisions—now are all connected, creating the IoT. The premise behind the IoT is that all these devices and objects are collecting and sharing data. This massive aggregation of data ("Big Data") can be automatically analyzed by computer algorithms (artificial intelligence, or AI) to determine identifiable patterns that can eventually be leveraged for more efficient, effective use of the individual objects and systems.

That same concept can be applied specifically to your hospital building through the "Internet of Buildings," or IoB. More than any other building type, hospitals have a significant number of potential smart devices, building systems, clinical equipment, and other leading-edge technology that can be connected, providing countless opportunities for workflow and systems to be more efficient and easily controlled. Everything from window shades to light switches to televisions and thermostats can exist in harmony with conventional building systems, information technology systems, and clinical systems on one unified network.

However, while designing your hospital to achieve this level of connectivity has many benefits, it also opens your facility to greater vulnerabilities. Each device that is connected to your network represents a potential intrusion point from a cyber security perspective. Often, since these less-technical devices wouldn't fall under their purview, your IT department may not even be aware of certain access points to your network.

Holistic approach to cyber security

Protecting a hospital's complete cyber infrastructure from malicious attack involves taking a holistic approach to cyber security. This requires recognizing that creating a secure cyber infrastructure involves more than protecting the computers and tablets in your hospital. It starts with the planning approach of the hospital itself.

Because of the IoB, planning of IT, building systems, and clinical equipment can no longer be carried out in silos. There must be a single, unified process that considers those systems holistically. (Related video: "Achieving transformational technology in healthcare.")

As the connectivity of devices and objects in their building grows, many hospitals also are utilizing cloud-based storage. Shifting the storage and processing of sensitive medical data to a third-party cloud provider allows hospitals to outsource portions of their network security as well. By storing electronic medical records and hospital servers in a cloud environment, the data is protected by the cloud provider's world-class experts in cyber-security—a level of expertise that few hospital systems can match. In addition, any intrusion that could come through a device on the IoB at the local level would be impeded from accessing important patient data because of improved network segmentation.

However, this solution won't be the right fit for every hospital and the decision to have portions of your network be cloud-based or on premises involves multiple considerations.

Summary: *With so many systems with network connections—from audio/video systems to security systems to clinical equipment—your hospital may have hundreds of different types of devices that utilize some type of connectivity. Recognizing this vulnerability and expanding your concept of cyber security to holistically include all these potential threats is the first step in creating a more resilient hospital cyber infrastructure.*

Resiliency requires vigilance

While healthcare resiliency may seem like nothing more than a catch phrase, achieving it is paramount for facilities to be able to care for their patient population regardless of disaster or threat. And when patient safety and hospital functionality are at stake, there's no room for cutting corners.

Hospitals would be well served by consulting with experts to receive outside perspectives on each of the five key areas of healthcare resiliency covered in this guide. However, when you're undergoing a facility or vulnerability assessment, seek consultants and engineers with a dedicated healthcare focus. The healthcare industry is unlike any other in its demands, and a healthcare-related specialist versed in MEP and structural infrastructure, physical security, or cyber security can better provide your hospital with the exact resources and insights needed to move forward and implement mitigation actions to remedy vulnerabilities.

True healthcare resiliency, however, doesn't stop there. It should be an ongoing process that is continually assessed and reviewed alongside a consistent education and training program for hospital staff.

While it might be impossible to prepare for every harmful scenario that might come your way, with the proper insights and expertise you can create a hospital that is as best prepared as possible for today's numerous threats.

*****

Examine resiliency in terms of healthcare's responsibility to the global community in the IMEG executive guides, "Enhancing the Quadruple Aim through Data-driven Decisions in the Built Environment" and "Decarbonization in Healthcare: A Practical Approach for the Built Environment."

For more information, contact:

Eric Vandenbroucke, PE, LEED AP
IMEG Senior Director of Healthcare
630.753.8512
Eric.J.Vandenbroucke@imegcorp.com

IMEG

Resiliency-related podcasts

Acuity Adaptability and the Future of Healthcare

CPTED: A Holistic Strategy in the Growing Quest for Safer Buildings

Data is the Key to Getting More Help from Your Building

Decarbonization in Healthcare: Why It's Needed, How to Get Started

Microgrids: Taking Emergency Power Beyond Code and Beyond Carbon

The Quadruple Aim and the Built Environment:

- Part 1: Healthcare's Dynamic Duo
- Part 2: Improving Population Health
- Part 3: Reducing the Cost of Care
- Part 4: Enhancing the Patient Experience
- Part 5: Improving Provider Satisfaction

The FUTURE. Built Smarter.
AN IMEG PODCAST