Since January 2020 Elsevier has created a COVID-19 resource centre with free information in English and Mandarin on the novel coronavirus COVID-19. The COVID-19 resource centre is hosted on Elsevier Connect, the company's public news and information website.

Elsevier hereby grants permission to make all its COVID-19-related research that is available on the COVID-19 resource centre - including this research content - immediately available in PubMed Central and other publicly funded repositories, such as the WHO COVID database with rights for unrestricted research re-use and analyses in any form or by any means with acknowledgement of the original source. These permissions are granted for free by Elsevier for as long as the COVID-19 resource centre remains active.
The planning and management of emergency incidents and conditions that healthcare organizations face daily come in many sizes, shapes, and colors. While some of these situations are intentionally created by man, others result from unintentional accidents, and still others are weather related. Each and every day, facilities react to a variety of emergency conditions.

Emergencies can be divided into internal and external situations for the purpose of this text. Regardless of the nature of the emergency, the organizational response will be quite different when the emergency condition exists within the facility from when it occurs at some distant location. The actual emergency response programs of healthcare facilities indicate that much more effort has gone into a prepared response to external emergencies than to internal emergencies. Exceptions can be found in the areas of fire safety and bomb threat programs, in which various regulatory and accrediting agencies have considerable involvement. A general list of situations that require emergency planning is difficult to compile; however, the situations listed in Table 42-1 should serve as a starting point, depending on the geographical location and type of patient care facility. The media and healthcare management publications have reported case histories for all of these listed emergency situations.

**BASICS OF EMERGENCY PLANNING**

Patient care facilities should perform a hazard vulnerability analysis (HVA) to identify potential emergency events that have the potential to impact the ability to meet a demand for services. In reviewing the list of potential emergencies, security practitioners should divide these situations into two categories: those that are most likely to occur and those in which the security protection system will be involved most extensively.

Security activity at the facility will be fairly standard if the emergency occurs away from the facility (external); that is, involvement will be in the general areas of access control (people and vehicles), information dissemination, and the procurement of supplies and equipment. The security response will primarily be a support role in the care and treatment of patients. A different involvement is indicated when the emergency situation occurs within (internal) or in the immediate area of the healthcare facility. As a general rule, the plan for security response to any emergency should be based, as a foundation, on everyday security safeguards and organizational resources in place. In other words, handling emergency protection needs should be viewed as an extension or expansion of the regular day-to-day security program. When facilities develop complex emergency plans that greatly differ from the normal handling of patients and basic pathways, confusion and inefficiency may result when the plan is activated. It is understood that circumstances may, however, dictate such changes. A case in point is the casualty triage receiving area. If this activity is moved from the normal triage location to another location, supplies and equipment must be moved, and police officers, firefighters, ambulance drivers, and facility personnel must be reoriented to respond to a new and perhaps unfamiliar location. The protection management plan then also becomes more complex and often unnecessarily burdensome.

---

**Table 42-1: Situations Requiring Emergency Planning**

| Manmade         | Accidental          | Natural       |
|-----------------|---------------------|---------------|
| Bombs/arson     | Fires               | Earthquakes   |
| Strikes/pickets | Hazardous materials | Hurricanes    |
| Terrorism       | Construction        | Snowstorms    |
| Gangs/mobs      | Utilities failures  | Tornadoes     |
| Civil disturbances | Transportation incidents | Floods |
| Pandemics       |                     |               |
| Active shooter  |                     |               |

---

*Originally from Colling R, York TW. Hospital and healthcare security. Boston, MA: Butterworth-Heinemann; 2010. Updated by the editor, Elsevier, 2011.
Federal Government, The Joint Commission, and International Association for Healthcare Security and Safety

The whole issue of healthcare emergency management took on a new look and new emphasis as a result of the September 11, 2001, terrorist attack. The major change and impact of this event was to significantly interject federal and state government into emergency planning and response for everybody, including healthcare. Following the massive federal initiative, The Joint Commission (TJC) made changes in their approach to emergency management. In 2009, it created a new, independent section for addressing the emergency management accreditation requirements. This subject had formerly been part of the Environment of Care.

The two main areas of healthcare emergency management receiving significant and increased attention are serving the medical needs that involve a medical surge capacity and the sustainability of the healthcare organization to function in their role with little or no outside support (i.e., utilities, supplies, food, etc.). In addition, it has become mandated that healthcare provider organization emergency planning must include other community and regional entities in an integrated and coordinated effort.

The term emergency, as used in context of the healthcare provider organization, can be any event that disrupts patient care services. Some emergencies are temporary and somewhat unremarkable relative to their impact on the organization, and others can be of a permanent and disastrous event that can completely shut down the facility. A strong wind may cause property damage, with little impact on patient care; however, in contrast, a flash flood may force immediate and complete evacuation of the facility for a period of time as in the case in Houston, Texas, in 2005. Also in 2005, Hurricane Katrina and Hurricane Rita caused irreparable damage to hospitals in New Orleans and Cameron, Louisiana.

A major question that avoids a validated and definitive answer is “How prepared are the nations’ hospitals to deal effectively with catastrophic emergencies?” The private sector maintains approximately 90% of the nation’s healthcare delivery capacity, but has not followed the efforts of federal healthcare facilities to reduce vulnerability through design and construction. Despite their efforts, the federal healthcare sector has been characterized as the weakest link in the homeland security chain.1

The International Association for Healthcare Security and Safety (IAHSS) has developed the following basic industry security guideline relative to healthcare emergency management.

Hospital Leadership. The first steps in developing plans and programs to manage emergencies include the setting up of a work group (a multidisciplinary committee). This work group would include representation from the Medical Staff, Nursing, Risk Management, Facilities, Security, Safety, and others deemed appropriate. In the past the Director/Manager of Security was often the person who was given the responsibility to lead this group. Today, it is somewhat common for the hospital to staff the position of Emergency Preparedness Director. Table 42-2 shows the results of a recent study of different hospital
positions that have the leadership responsibility for the Emergency Preparedness Program.

Phases of Emergency Management. The TJC views emergency management in four phases that take place over a period of time. These include: mitigation, preparedness, response, and recovery. The mitigation and preparedness phases generally occur before an emergency event, whereas response and recovery are phases that take place after the event. The details of activities and actions required relative to these four phases should be captured in the organization’s Emergency Operations Plan (EOP). Once the EOP is completed, it must be tested through emergency response exercises and drills to evaluate its effectiveness. Thus, emergency management is an ongoing process of planning, directives, evaluation, more planning, added or changed directives, etc.

Emergency Preparedness Drills

Emergency drills are required by TJC and other accreditation or regulatory agencies. Every accredited facility must conduct drills and prepare a written report evaluating each drill.

People who have been assigned to observe specific aspects of the plan must meet after the drill to determine the plan’s effectiveness. It is generally agreed that observers should be people from outside the organization when possible. They traditionally come from state agencies, offices of emergency preparedness, medical societies, or other medical care facilities. Drills serve a very important purpose, and they must be conducted with all the realism possible. It is extremely difficult, however, to rehearse certain parts of an emergency disaster plan when the facility is open and conducting routine, everyday business. One of the most difficult elements to practice is that of people and vehicle traffic control. It is not practical to restrict visiting or to turn away patients who have an appointment. Physicians and the community will not accept the curtailment of normal activities for a drill.

Real progress has been made in the last few years for healthcare providers to integrate their emergency management planning and operations with other community resources. This area-wide coordination has greatly improved the ability of a community, working together, to respond more effectively to the vast array of different types of emergencies both large and small. It is therefore natural to conduct emergency exercises and drills, both organization-specific and community-wide. There will continue to be more and more federal involvement in community emergency management through control of grants and legislation. An emerging federal program is the Homeland Security Exercise and Evaluation Program (HSEEP), which develops standards for hospital exercises. Many hospitals already use HSEEP methods to conduct their drills in conjunction with community public safety agencies.

An example of a large-scale mass casualty community drill was recently conducted by the University of Wisconsin Hospital and Clinics, which was dubbed “Operation Red Dragon.” It was the largest mass casualty drill to be held in Wisconsin state history. Members of the 415th Chemical Brigade of the U.S. Army Reserves with 170 participants and the urban hospital network were involved in the drill. Members of the brigade played victims and the hospital tested its state-of-the-art decontamination system. The primary goal of the exercise was to test communication between the military and hospitals in the event of a large-scale incident.

Another example of healthcare organizations integrating their emergency response planning with other community resources is the Special Operations and Response (SOAR) trailer as part of Carolinas HealthCare System (CHS), headquartered in Charlotte, North Carolina. The trailer Emergency Operations Center (EOC) is shown in Figure 42-1.

The specially designed 16 foot trailer was created to provide communications and tactical support to security, law enforcement, and firefighters at remote sites throughout the CHS service area. In addition to its onboard communications (HAM, UHF, VHF plus connections for standard/satellite phones), the trailer allows

| Hospital Position | Percent of Survey Group |
|-------------------|-------------------------|
| Emergency Preparedness Director | 33% |
| Security Director | 20% |
| Safety (Director, Manager, Office Coordinator) | 13% |
| Facilities Management Director | 11% |
| Risk Management Director | 5% |
| Other | 18% |

FIGURE 42-1 The CHS Mobile Emergency Response Unit.
for recharging of radios, respirator batteries, and similar equipment. Plans are to install additional equipment, which will have the ability to create ID badges on-site for personnel responding to the event.

**Incident Command System (ICS)**

An ICS is a basic component of the HCF’s EOP. An ICS is the combination of personnel, procedures, communications, equipment, and facilities operating within a common organizational structure directing the response and activities in managing an emergency incident or condition. There are two major models of incident command structures in use in the majority of U.S. hospitals. One is the federal model, developed by the Office of Homeland Security, which is the National Incident Management System (NIMS), and the other, Hospital Incident Command System (HICS), was developed by California’s Emergency Medical Services Authority. The HICS model is specifically directed to hospitals for incorporating a command structure, defined responsibilities, and common terms. It should be noted that the original California model was named Hospital Emergency Incident Command System (HEICS), and in 2005 the word Emergency was dropped to become HICS. The NIMS model is a somewhat broader model (nonspecific to type of industry or organization) of practices in emergency preparedness and response to a national framework of managing critical incidents. There have been recent changes in the HICS model to more closely align, yet to be hospital-specific, to the broader NIMS model.

**NIMS and Federal Funding.** An important element of NIMS is their publication, “FY 2008 and 2009 NIMS Implementation Objectives for Healthcare Organizations.” Federal grant funding for hospitals through Assistant Secretary for Preparedness and Response (ASPR) and Health Resources and Services Administration (HRSA) require meeting a minimum number of the NIMS objectives (activities).

There are 14 NIMS objectives for healthcare organizations (FY 2008 and 2009) that are grouped under five major categories. These categories are:

- Adoption (of NIMS)
- Preparedness Planning
- Preparedness Training and Exercises
- Communication and Information Management
- Command and Management

**PRIMARY MAN-MADE EMERGENCY EVENTS**

**Fire Prevention and Control**

Security along with facility safety services has a major responsibility in fire prevention control regardless of whether a fire is man-made or accidental. Fires in U.S. HCFs have decreased in the past decade; however, some 10% of HCFs have suffered a fire loss at some time in their history. Although this is a much lower rate than that of general industry, HCF fires can mean the loss of human life as well as significant financial loss. The term *fire prevention* refers to the everyday activities that eliminate hazards and prepare people to react properly should a fire actually occur. In this discussion, the term “fire control” pertains to the basic organizational reaction to an actual fire. Both fire prevention and fire control should be addressed in the organization’s fire safety plan.

Patients being treated range from those who can move freely without help to those who cannot be moved without life-support equipment. Also, infants, children, behavioral health patients, and the elderly present unique requirements that must be considered in the fire plan. The elderly, especially those in nursing homes, are a particular concern. More deaths occur each year in facilities that care for the aged than in all other healthcare facilities combined. Not only are these facilities minimally staffed, but a high percentage of the elderly must be assisted during evacuation. The aged are generally slower to react to emergencies, and they often react unpredictably. An additional complication is that the products of combustion, even in small quantities, are often more fatal to older people.

**Fire Safety Programming.** A fire safety program can be viewed as five basic elements: (1) prevention, (2) detection, (3) containment, (4) evacuation, and (5) extinguishment. These elements chronologically define a standard organizational response to a fire threat.

**Fire Prevention.** Prevention encompasses the activities of the fire safety program that occur before an actual fire, including the identification and correction of fire hazards, fire control planning, employee and occupant education, design and specifications, equipment tests, drills, and fire department liaison. Absolute fire safety is unattainable because it is impossible to exclude from the facility everything that burns and all sources of ignition. Facility inspections are conducted by all kinds of inspectors, including representatives of insurance companies, CMS, TJC, city building departments, state and city health departments, and fire department personnel. Some of the best inspections, however, are those conducted by organizational personnel. If they are conducted properly, a continuous, everyday fire inspection program is accomplished. Security officers on their rounds should note and/or correct fire hazards they see or that are brought to their attention by others. Security officers on rounds should be particularly alert for people smoking in prohibited areas. Officers should correct and report doors left open that should be closed, obstructions to egress paths, careless use of oxygen cylinders, and other fire safety violations. If a hazard cannot be corrected on the spot, officers can, through proper reporting, initiate administrative action.

**Detection.** Automatic early warning smoke detection and pull box systems are typical in many facilities
since regional and national codes generally require this equipment for inpatient facilities. In many healthcare facilities, detection equipment transmits a signal directly to the fire department, while at the same time alerting facility personnel. Smoke detectors use sensing units that respond to the presence of products of combustion that result from a fire. Other types of detectors may respond to heat or flame. When the threshold is exceeded, the sensor is activated. Most HCF fire detection systems use a combination of devices due to the varied situations the medical care environment presents. Activation of a fire detection device may also control various items of equipment; it may activate fire extinguishing equipment and air-handling machinery, send elevators to predetermined locations, and release magnetic hold-open devices on doors.

**Containment.** The third element of the fire safety program is the containment of smoke and fire. The objective is to contain the fire in the room or area of origin. When this is not possible, the goal is to provide successive levels of defense or areas of refuge from the fire. The five basic areas of fire containment are sometimes referred to as the unit concept. The units are the room, the compartment, the floor, the building, and the exits, all of which have a distinct function in the fire protection features of the building.

- **Unit 1.** The room — the smallest unit — is the first line of defense. The function of Unit 1 is to provide the first barrier against the passage of smoke. The more effectively a room can be sealed, the better job it will do in containing fires.
- **Unit 2.** The compartment is the second level of defense. The intention is to provide at least two areas of refuge on every horizontal plane of the facility. When an area must be evacuated, the initial movement is horizontal rather than vertical. The Unit 2 compartment is created by smoke and barrier walls.
- **Unit 3.** The floor, or floor assembly, is the next level of containment. The function of the floor assembly is to prevent the spread of fire and smoke from one floor to another.
- **Unit 4.** The building is the fourth level of protection. For the building to remain structurally intact for a period of time, it should maintain structural components that offer minimum contribution to any fuel load and that can withstand the effects of a fire within the facility.
- **Unit 5.** The exit path is the final unit in this concept of fire protection. At least two remote exits must be provided on each floor or fire section of the building. Exits do not need to lead directly to the outside. They can include egress to interior stairs, exterior stairs, horizontal exits, ramps, and exit passageways. Fire containment can also limit the air needed to sustain combustion. The heat and smoke from a fire generally rises as a result of the buoyancy created by the heated gases. The smoke and heat will also seek out a path to the outside air. If they cannot continue to rise, the smoke and heat will descend back to the floor level.

**Evacuation (Relocation).** The fourth component of the facility fire safety plan is relocation of patients, visitors, and staff. The Life Safety Code — through its standards for exit capacities, types of exits, travel distance, door specifications, and similar details — ensures the necessary means of egress from a medical care facility during an emergency. It is the healthcare staff, however, who is responsible for moving any patients who are in imminent danger to a safe location. In hospitals, many occupants are incapable of self-preservation. This fact is recognized by the Life Safety Code, which places the main responsibility for patient safety on the HCF staff.

Total building evacuation, as a measure of last resort, can and does occur. Patient relocation between smoke-protected compartments on the same floor is usually an adequate first step. Following the unit concept principle, the evacuation plan’s first objective is to move patients to a safe compartment. At this point, it must be determined whether to continue horizontal evacuation or whether vertical movement (to another floor) is necessary. Wheelchairs and carts are useful and often necessary for relocating patients, but they may not always be available at the time and place of need. Blankets are always available, and security professionals generally agree that they can be the most important pieces of equipment on hand for evacuation. Elevators should receive special consideration in the fire evacuation plan. Generally, plans prohibit the use of elevators for egress or relocation purposes because of their recall features, which are normally activated in a fire condition. An elevator may stop at the wrong floor, exposing its occupants to the fire. On the other hand, high-rise hospitals present unique problems that may require the use of elevators for vertical relocation under controlled conditions. In addition, the fire department may need to utilize an elevator for their firefighting purposes. Generally a building of more than seven stories is considered a high-rise, and is the limit of most fire department ladders. A vertical evacuation plan is mandatory for high-rise buildings. One or more elevators in a wing removed from the fire area may be used to transport patients to another floor much more quickly and with fewer possible medical complications than when patients are carried down a stairwell.

It is noted that not all evacuation of patients will be related to a fire situation. Evacuation for any number of emergency conditions such as weather disasters, loss of infrastructure support, bomb threats, and so forth may require moving large numbers of patients. The unique operational issues of evacuation under different conditions should be covered in the organization’s EOP. In terms of providing evacuation plans for different types of patients, the forensic patient must also be part of the planning effort.
Extinguishment. The last element of the hospital fire safety program is extinguishing the fire. The suppression of fire by staff is achieved manually or by automatic suppression systems required for all new construction. The automatic sprinkler system is the most common of the automatic suppression devices. The automatic sprinkler system also acts as an alarm device because all systems are installed with water-flow sensors that activate an alarm when water is flowing in the pipes. The sprinkler is activated by a thermally sensitive element that automatically releases water at a predetermined temperature. Other piped extinguishing systems include water spray, foam, carbon dioxide, dry chemical, Halon, and newer, environmentally sensitive, clean agents. The standpipe and hose system, found in most U.S. medical care facilities, is used to provide quick and convenient water streams. This system is most generally used by fire departments or trained fire brigade personnel. It is not uncommon to eliminate the hose at the valve locations. The rationale for this is that most fire departments supply their own hose. Further, there have been reports of vandalism by opening the valve a little and allowing the hose in the cabinet to fill slowly with water. The hand-held extinguishers used in medical care facilities are primarily 2.5 gallon, stored-pressure water extinguishers, carbon dioxide extinguishers, and multipurpose (ABC) extinguishers. The type of extinguisher at any given location is predicated on the primary type of hazard involved.

Employee Reaction to Fire Events. Proper employee reaction to a fire is one of the fundamental factors in saving lives and property. Fire safety is a race against time, and the action taken within the first few minutes can make the difference between a minor fire threat and a tragic disaster. Because employees must act almost instinctively when fire breaks out, detailed instructions are seldom remembered. The following simple steps, expressed through an easily remembered acronym, are widely used in healthcare facilities:

- Rescue those in danger.
- Activate the alarm.
- Contain the smoke and fire.
- Evacuate and Extinguish.

Fire Safety Training. Any employee could be the one who discovers a fire or who is the first to arrive at the scene of an alarm. The high rate of personnel turnover in medical care facilities and the difficulty of retaining procedures that are not used routinely require continuous in-service and new employee training classes. Fire safety training is usually the responsibility of the Safety Administrator. Training can include posters, contests, in-service training, and fire drills. One of the obstacles faced in fire safety training is that little uniformity exists among facility fire plans. Because of the transient characteristic of medical care staff, an individual may work at two or more facilities at the same time. Organizations and facilities all have unique characteristics that require special fire planning; however, especially within a given locality, common fire plan components among facilities would reduce training time.

Basic Security Fire Response Considerations. Security’s role in a fire situation is part of the overall facility fire plan, which includes:

- Ensuring that responding fire department personnel gain access to the facility complex, buildings, and internal areas. This may require unlocking gates or doors, holding elevators, turning on lights, and even escorting fire personnel to the fire area.
- Controlling traffic, including vehicular traffic and people on the perimeter of the fire scene as well as the emergency operations areas.
- Assisting with the evacuation process if necessary.
- Assisting emergency personnel throughout the emergency.
- Securing the area after the conclusion of the incident. A fire watch may be required for some time after the fire has been extinguished.
- Providing security officer fire training. This training goes far beyond the general employee fire training previously discussed. Security officers are not only the first responders in many cases. The action taken in the first few minutes will bear directly on the outcome. Initial concerns involve sizing up the situation for personal safety, sounding an alarm, containment, and controlling the fire. Beyond these basics, there may be evidence that should be protected or conversations that should be noted and retained. Arson does happen in medical care facilities. Security officers must notice if someone has an unnatural or unusual interest in the fire. In short, security officers may be exposed to too much information in the initial moments of a fire — information that must not go unnoticed or it may be lost forever.
- Preparing appropriate documentation of the fire incident.

Bombs and Bomb Threats

Bomb threats are a reality for medical care organizations. Although the number of threats has decreased over previous years, a significant number still occur. One of the unique features of the bomb threat is the guessing game it forces the threatened organization to play. Is it real or is it a hoax? Where do we search? Is evacuation necessary? These basic questions become the framework of the facility response plan. The plan must be flexible to the degree that the information received can be applied to these questions at the time of the threat crisis. A bomb can be described as any explosive, incendiary, or gas-filled container. Many chemicals can be used to make a bomb, and most chemicals are easily obtainable. Dynamite can be purchased or stolen from construction sites. Ammonium nitrate is sold in stores...
that handle fertilizers. Potassium nitrate and black powder can be bought at shops that supply chemists or hunters. Pipe bombs are commonly used by amateur bombers. These bombs are made from an ordinary pipe capped on both ends and generally filled with black powder.

The Bomb Threat Plan

All HCFs should have a written bomb threat plan. Each plan is unique to the specific facility; however, the basic steps of bomb threat programming can be categorized as follows: (1) prevention, (2) establishing authority, (3) receiving the threat, (4) searching for the bomb, (5) evacuating the building, (6) terminating the emergency, and (7) documenting the threat.

Prevention. The first area of concern is the preventive steps that can be taken against a bomb situation. These steps are the same security safeguards that should be in everyday use to protect the organization against other security risks. In other words, the proper functioning of the day-to-day protection system is the first line of defense against the bomb threat. To be more specific, locking equipment rooms, switchboard rooms, utility closets, storage areas, and so forth can help reduce the problem. Limited access, access controls, noting suspicious people and vehicles, and providing emergency equipment are all part of the everyday protection system.

Establishing Authority. One of the most important aspects of properly managing a bomb threat is to specifically establish organizational authority. As basic as this point seems, it is a fundamental deficiency of many healthcare organizations. Authority and responsibility for handling the initial crisis must be designated to a position that is readily available 24 hours a day. Logical choices would be the nursing supervisor, the house officer, or the security shift supervisor. The various field resources brought into play during this type of emergency must know to whom they must report the information, and answers to questions must be immediately rendered. It may be necessary to activate the ICS to properly manage the bomb threat situation.

Receiving the Threat. The bomb threat can be received in numerous ways. The most common method is by telephone, and the most common recipient of such information is the switchboard operator. Telephone operators and others who are likely to receive these calls should be trained to keep the caller talking as long as possible and to ask key questions, such as where the bomb is, when it will go off, why it was placed, what kind of bomb it is, and other questions that may keep the caller on the line. The person who receives the call should make notes or activate a recording device. Not all threats indicate that a bomb has been placed somewhere in the facility. The threat may indicate a bomb “will be” placed in the facility. When this type of threat is received, access controls must be expanded and the organization may decide to examine property being brought into the facility.

Searching for the Bomb. The bomb threat information received must be communicated to the designated authority within the organization, who in turn initiates the notification system. The first step in the notification procedure must always be to notify the appropriate law enforcement authority. In most cases, the law enforcement authority and facility management will decide jointly the type and extent of search required. It is not practical or possible to conduct an all-out search in every case, which includes everything from checking every patient’s belongings to removing all suspended ceiling tiles and all ventilation grille work. It could take at least a day or two to completely search a facility. It is presumed that people who carry bombs are well aware of the danger of premature detonation, and therefore in most cases they will want to get into the facility quickly and to get out even more quickly, which generally precludes an elaborate hiding process. If sufficient organizational personnel are available, the search should be conducted by staff rather than by the police or fire department. The proper role of the outside support agencies is to assume control if a bomb or suspected bomb is located. Employees should conduct the search for two basic reasons. First, staff are in the best position to know what belongs and what does not belong to a given area. Staff are more knowledgeable of the layout of the facility and have the capability to enter locked or controlled areas or know how to obtain access.

The use of in-house personnel to search avoids unnecessary confusion and minimizes disruption. Patients do not welcome a police officer, or a security officer, searching their room at 2:00 a.m. The search can be emotionally upsetting, and the reaction could very easily be panic. Many experts believe that bomb threat callers are frequently interested in stirring up as much activity and causing as much disruption as possible. Thus, one objective of a bomb search is to carry out the search in a smooth, routine manner, while taking every threat seriously. In bomb threat situations, the administrative person handling the threat may decide to advise only selected staff and patients. In general, patients should not be told of the problem unless absolutely necessary. Experience has shown that patients often set off a chain reaction that is detrimental to the entire process. Patients may respond by calling their families. In turn, the family may decide to come to the facility or call the facility for detailed information. This reaction can tie up needed communications lines and hinder response capabilities.

Whether a search is full or partial, areas of responsibility must be assigned. In some plans, the search personnel are assembled as a group so that the search coordinator can relate to them the information received and assign specific areas to specific personnel. In other
plans, this information is communicated by telephone or through a public address system with a code term such as “Mr. Search” or “Code Green,” or via electronic means. A problem that must be taken into consideration is the staffing pattern of the facility. When all departments are fully operational, the facility can be more easily and quickly searched than when departments are closed and locked. During the nonoperational period, security, maintenance, and environmental services personnel may be assigned an expanded role in the search effort. Floor plans that have been divided into specific search areas are used in some facilities. Personnel are given a map of the area for which they are responsible. In other organizations, these assignments are made from an administrative checklist that defines the areas. However the parameters of the search are defined, the person responsible for searching a given area must always report back to the control center when the search has been completed. The primary concern is for personal safety rather than property. Thus, a threat at 11:30 p.m., when minimal staff is on duty, may preclude searching all areas. It may be that closed areas such as food service, business and accounting areas, administrative offices, maintenance shops, medical record areas, and so forth receive only cursory examination. The occupied areas of the facility should be searched more thoroughly. Some controversy exists over the use of two-way radios during a bomb search. It has been suggested that radios should not be used because a bomb might be constructed to detonate in response to the transmission of radio signals. However, most experts believe that this possibility is extremely remote. In almost all situations, the radio system is active before the bomb threat was received and would have already detonated the device. The benefits of two-way radios during emergency operations support their use unless specific information is received to the contrary.

**Evacuating the Building.** If the search produces a bomb or a suspected bomb, the cooperative efforts of security and public safety agencies come into play. Facility employees should never touch a suspected bomb. The investigation and removal of any suspect object is the responsibility of the public safety agency. Security’s basic function is to seal off the area and to commence evacuation if necessary. The decision to evacuate rests with the facility administrative authority working in cooperation with the public safety agency involved. The evacuation of employees from a given work area presents no serious problems. Any plan for evacuating patients, however, must take into consideration the magnitude of the problems involved in moving the helpless and the seriously ill and the medical complications that may result. The extent of the evacuation is another decision that must be made quickly, based on the specific situation. A safe distance for evacuation is generally considered to be a 200 foot radius from the suspected object, including the floors immediately above and below.

**Terminating the Emergency.** An important part of the organizational reaction to the bomb threat is the decision to end the response. All people who were notified of the receipt of the threat should also be officially informed that the organization is resuming normal operations. In other words, the activity generated by the threat should not simply be allowed to trail off. After the threat is over, environmental services, maintenance, and security departments should brief the next shift of employees in their respective departments. In the normal course of their activities, these employees may observe something of importance that was overlooked during the earlier official search.

**Documenting the Threat.** The last step in bomb threat procedure is to document the incident for future reference. This task is usually assumed by the security or safety department. Regardless of who prepares the documentation, it is the responsibility of the person in charge of the threat incident to make certain that this important task is completed. The security report generally focuses on recording the facts of the situation. An additional administrative report that critiques the bomb threat response may be appropriate. The analysis may reveal deficiencies that require plan modification or further employee education.

**Strikes and Picketing**

A real test of a facility’s protection plan comes when the facility faces a strike or picketing situation. A strike occurs when some of the organization’s employees, commonly represented by one or more unions, refuse to work as a protest against a serious grievance or a failure to negotiate a mutually acceptable contract. Picketing refers to the placement of people around the exterior of the facility for the dual purposes of informing the public of alleged problems and curtailing deliveries of supplies and equipment. The primary purpose of a strike is to create hardships for the organizations, weaken their bargaining position, and resolve the dispute in favor of the protesters. The hardships may include disruption of patient care, intimidation of nonstriking staff, loss of revenue, damaged or stolen property, negative community reaction toward the facility, and injury to persons. An organization need not be unionized to become the focus of a picket line. Picketing may be set up as a result of a strike or for the purpose of attempting to force the organization to recognize a collective bargaining unit. The immediate effect of a picket line is that union drivers may refuse to cross the line to make deliveries. In the initial stages, nonunion drivers will often cross the picket line until threats are made or physical violence occurs.

**Strike Control Team and Strike Action Committee.** During a strike, an organization must have a unified command structure. The organization’s chain of command dictates the position that will be responsible for strike control operations. The strike
control team should operate out of a strike incident command center so that all employees and outside support groups know where to deliver information or seek direction. A strike action committee should be formed by the head of strike operations to represent the various operating units of the facility and to function primarily in the pres trike preparation phases. Once a strike is underway, the committee will rarely be needed; however, it may meet periodically as a communication tool to keep operating units advised of the situation.

Nonstriking Employees. The nonstriking employees are the basic resource for continuing patient care and ensuring a successful conclusion to the labor action. It is extremely important that the administration support nonstriking employees in every way possible. On the day the strike begins, all nonstriking employees should attend a briefing meeting designed to update employees on logistical matters, exhibit the administration's support and appreciation of the staff, and reassure employees. The employees should be told to expect harassing telephone calls. These calls generally threaten not only the employees, but also their families if the employees return to work. It may be difficult for administration to talk about this situation because administration generally wants to avoid negative issues. However, forewarning employees can mitigate the initial shock of these types of threats. Nonstriking employees are also vitally concerned about the protection of their vehicles while they are at work. Because experience has shown that vehicles are a major target of strikers, this concern is certainly valid. High priority must be given to this protection responsibility.

Initial Stages of the Strike. The first day or two of the typical healthcare-related strike is generally peaceful and uneventful. The strikers are in a fairly good mood and enjoy talking with one another. The greatest number of picketers is on hand in the early stages of a strike, except for major rally events when the union tries to show a high degree of support. Inside the facility, the staff's initial reaction is enthusiastic support for the organization. As the strike continues, both picketers and staff will exhibit frustration, disappointment, and exhaustion. After a few days, when the facility seems to be functioning well, the strikers begin to wonder whether efforts are meeting objectives. Their reaction may be to step up harassment. Incidents of intimidation, property damage, and other problems sometimes begin to appear. Another tactic that may occur and will affect the facility is a secondary boycott by suppliers and vendors. This illegal activity usually occurs much later in the strike, but it should be anticipated during early planning.

Picket Lines. A major purpose of the picket line is to discourage employees from crossing the line to report to work. When the picketers see that employees are not being sufficiently discouraged and do cross the line to work, confrontations sometimes begin to take place. It is at this point that threats and acts of violence often occur. Administrators and supervisory personnel should be on the grounds during shift changes to support arriving personnel and to observe any incidents that might occur. Employees arriving to work are encouraged when they see the upper echelon there to support them rather than sitting safely behind their desks. Most healthcare facilities have a built-in security vulnerability that can become an asset during picket activities: a multitude of entrances and exits. For the duration of the strike or picketing, as many of these access points as possible should be open for employee use. The more entrances that are available, the more difficult it becomes for the picketers to cover them all. The law states that picket lines shall not restrict the right of people to enter and leave the facility. Despite this provision, thousands of incidents on record involve injury to people and destruction of property during picketing. In coping with this situation, it is a common mistake to assume that law enforcement agencies will maintain law and order. Unfortunately, for a variety of reasons, police protection is not always at its best at such times. The healthcare organization has a responsibility to provide for personal safety and to protect its assets. The security department will necessarily play a strong role in achieving this objective. Several days before the strike, there should be a thorough inspection of the exterior of the facility to remove signs and other items that could be easily vandalized. One item often overlooked is sprinkler heads—a favorite target for picketers. Security personnel are generally deployed at the site of the picket line to show nonstriking employees and others who cross the line a high degree of protective support. Security's additional responsibility is to ensure that picketers stay off facility property, to prevent accidents, and to document evidence of wrongdoing. It is recommended that security personnel assigned to the strike detail be unarmed. A security objective is to be present but to project a fairly low profile, indicating that no trouble is expected. The type of trouble that might occur will not be deterred or corrected with the threat or use of a firearm. Security officers should be briefed by the administration and legal counsel just before they are deployed to the picket line. The basic message this briefing should convey is that officers must be professional. They must keep their eyes and ears open and their mouths closed. The officers should be reminded that they are representatives of the organization, regardless of their personal feelings about the situation.

Record Keeping. A step that must be initiated immediately when a strike or picket situation develops is to establish a strike control center. A major administrative mistake is to assume that the confrontation will not last long. This assumption makes it easy to ignore the central reporting and its record-keeping role until the organization is well into a prolonged strike. All information concerning activities and incidents related to the
labor action should be reported immediately to the designated recording location. All supervisory employees should be given the responsibility of reporting all incidents brought to their attention. A chronological record of incidents, including complete details, serves a variety of purposes, not the least of which is collecting the data necessary for legal actions. A consolidated central reporting concept will also serve as a clearinghouse to verify or reject rumors and to readily assess the situation. An important tool in dealing with and documenting strikes and picketing — and one that relates very closely to the incident recording function — is the use of photography. The task of photographing the labor action should be an assigned responsibility. Because camera equipment is often antagonizing to picketers, it should be used in such a manner that a minimum of confrontation occurs. The organization’s response to the labor action may require the unexpected expenditure of funds. Special arrangements may have to be made to procure supplies, obtain drivers and vehicles, authorize meals, use taxi services, authorize overtime, and the like. During times of the strike, the customary management controls tend to be loosened. Specific guidelines must be drawn up for these unexpected expenditures, and the individuals who authorize the use of funds must keep adequate records.

**Maintaining Supply Lines.** If it is to continue to carry out its mission, one of the first and most important steps an HCF must take during a labor action situation is to maintain a supply line. In most instances, a supply line requires the procurement of additional labor and vehicles. If vehicles are obtained from rental or leasing companies, it is usually only a matter of time before the rental agency demands the return of their vehicles. This tactic can be countered to some extent by having individuals rent vehicles from various agencies for one-time use. This procedure also proves valuable in avoiding harassment because the newly rented vehicle can be used to pick up supplies without being followed and subjected to threats, damage, or driver injury. Before picketing begins, the organization should contact all suppliers who make deliveries to the facility. The facility needs to know if nonunion or supervisory personnel will be available to make deliveries. It is better to pick up the supplies directly from the vendor or to have the order shipped to a temporary receiving site than to have confrontations between picketers and truck drivers. When truck drivers refuse to cross the line, their action supports and encourages the picketers. Because it is impossible for the facility to pick up the thousands of items it requires, particularly during a prolonged strike, off-site receiving areas can become necessary. Off-site receiving points should be well secured and generally require security officer coverage. Depending on the severity of the strike, the location of the off-site receiving point should be changed periodically. Organizations should consider using a truck parked in a vacant lot or other out-of-the-way place and simply off-loading from one truck to the other. If the loaded trucks are not brought to the facility the same day, security precautions are important. One HCF involved in a severe labor action had parked three trucks overnight in an abandoned section of a railroad yard, and all three trucks were fire-bombed. The picket line not only inhibits the free flow of deliveries but also affects the removal of items, particularly trash. An institution of any size will find that a tremendous volume of refuse can build up in a very short time. It is essential that facilities move quickly to dispose of this material or they may find themselves in violation of health and fire standards. Inspectors from various federal, state, and local regulatory agencies just seem to proliferate during labor actions.

**Terrorism**

To many U.S. citizens, terrorism was something that took place elsewhere — until the September 11, 2001, attack. Acts of terrorism, both internationally and domestically, continue to occur, albeit on a smaller scale. Those who claim to know, predict another large-scale attack on U.S. soil in the near future. The federal government continues to release information on how it is becoming better organized and better equipped to handle both domestic and international terrorism. If one looks at the record of the Transportation Service Authority with ever-changing plans and directions, it would give one a time to pause relative to how well the government is prepared. The color alert codes seem to be a fad in passing and little is heard in that regard, except in airport overhead announcements. It has been reported that the Department of Defense is gearing up to play a larger role in homeland security. Under their plan, three rapid reaction forces will be ready to assist state and local officials with large-scale emergencies by 2011. One is a 4,700-person unit built around an active duty combat unit stationed at Fort Stewart, Georgia. This may sound good, but it is the prevention of an emergency rather than the reaction to it that is of prime importance.

A question that continues to be asked is: Are hospitals a likely target for a large-scale terrorist attack? As one might expect, there are varying answers to the question. Lawrence Likar, a retired agent of the FBI, speaking at an annual meeting of the American Society for Healthcare Risk Management (ASHRM) at their 2006 meeting in San Diego, stated that the threat to hospitals is very low. Others claim that hospitals are at a high level of risk, as one criterion of the terrorist attack is to create a horrific event. A large-scale attack on a large hospital, perhaps even a children's hospital, would no doubt meet the terrorist objective. The general consensus of professional security administrators, however, is that the probability of a terrorist attack on a hospital is in the low to low-medium range.
Weapons of Mass Destruction. A topic receiving increased attention is that of WMDs. Within the realm of WMDs, there are five generally accepted categories of terrorist actions: biological, nuclear, incendiary, chemical, and explosive (B-NICE). Hospital emergency departments will generally be early, if not the first, responders. While military medical services may be a resource, in all probability they may not be mobilized in a timely manner to meet initial needs.

Biological and Radiological Weapons. The type of terrorist weapons is always at issue. It appears that a terrorist attack is more likely to be the use of a biological weapon. Anthrax and other dangerous biological materials are found in nature around the world, while weapon-grade nuclear materials are not readily available. It would be much simpler to disperse biological agents than to manufacture a nuclear weapon.

There is a growing concern that a terrorist’s weapon of choice may be a radiological dispersal device (RDD), which uses conventional explosives to spread radioactive materials. These devices, commonly referred to as “dirty bombs,” are not classified as a WMD as they do not usually produce the mass casualties of a nuclear device. The detonation of an RDD device serves a three-fold purpose: a blast and fragmentation generated by the explosion, the dissemination of radioactive material, and the fear and panic generated in the targeted area.

Hospitals do not present a large source of radioactive materials. These materials are in the form of powder (i.e., blood bank irradiator), wafers (i.e., gamma knife), and liquid (i.e., diagnostic uses). Even in limited amounts, the theft of radioactive materials from these sources is a potential threat deserving of proper security safeguards. Since there is a real danger in moving radioactive materials, it is likely that the theft of such materials from a hospital may in fact be used to construct a dirty bomb for detonation on-site (the hospital).

The Washington Hospital Center in Washington, DC has recently begun to install radiation detection units. These units will alert staff if someone who is contaminated with radiation enters the hospital. It is reported that testing will ensure that the units will differentiate between dangerous radiation and radiation used in cancer treatments. The units will also trigger an alarm if someone attempts to remove radioactive materials from the hospital.

The security safeguards applied against terrorist threats coincide with safeguards used against civil disturbances, that is, an expansion of the elements of the day-to-day security system in place.

Gang and Mob Activities

Gang and mob activities are different from riots and civil disturbances in that gangs and mobs generally focus on the hospital as the primary target of their actions. Medical care facilities have been the object of demonstrations, ranging from peaceful marching, sit-ins, the occupation of administrative offices, and the takeover of communications systems. The purpose of these demonstrations has been varied and has included such demands as free medical care and the reinstatement of terminated employees. These disruptive activities characteristically show a complete disregard for the rights of the medical care facility and for the negative effects on patient care. In general, hospitals prohibit the exhibition of gang colors or flashing signs. Most security professionals agree that a strong security presence and dealing firmly but fairly with gang members is the best approach. Too passive an approach usually escalates disruptive behavior.

Planning for Gang and Mob Activity. One of the most important points to consider when planning an organization’s response to gang and mob activity is the policy on arrests. Specifically, will arrests be made, and who will make this decision? Once the police have been called, the facility must be prepared to sign complaints and to follow through in prosecuting demonstrators if the police are unable to persuade them to leave.

Of the many mob activities directed against healthcare facilities, a demonstration against the Beth Israel Medical Center in New York many years ago is of particular interest to security practitioners. A group of people demonstrating under the banner of the Health Revolutionary Unity Movement disrupted services, and the hospital sought and obtained a court injunction prohibiting demonstrations within the hospital. The decision handed down by Justice Mitchell of the New York Supreme Court clearly stated that a medical facility is not a public place, and its sole purpose is to render medical care and treatment, for which a tranquil atmosphere is required. The opinion also stated that the demonstrators were in error when they justified their conduct on the basis of their constitutional right to freedom of speech and assembly. Although the case is more than 30 years old, other case law has supported these principles. Although the law supports medical care facilities in their defense against intrusion, injunctions take time, and facility protection still requires careful and detailed planning.

Civil Disturbances

The outbreak of rioting in the late 1960s presented a relatively new protection vulnerability for healthcare institutions. Hospitals had previously handled mass casualties, but the influx of casualties from rioting created new complications for protection services, including:

- Confrontations between police and rioters that often continued into treatment rooms
- Hostile visitors who demanded attention, disrupted activity, and destroyed property to obtain their objective
• Direct attacks on the facility, including firebombs and in one case a siege of gunfire

In short, HCFs ceased to be the neutral ground they had been in the past. During the 1970s, few, if any, civil disturbances involved hospital operations. In mid-1980, heavy rioting hit Miami, Florida. One hospital, Jackson Memorial Medical Center, was under siege for a few days as rioters burned and looted just outside the hospital’s perimeter. Security professionals learned three things from these riots. First, police and fire protection services may not be available as assumed or even as promised. Many facilities suffered extensive damage and disruption because the municipal protection services were stretched so thin that adequate protection could not be furnished. Every protection plan should therefore be predicated on the assumption that no external help will be available. Second, employees may be sympathetic to the rioters and their cause. Employee sympathy may be manifested in the theft of drugs and supplies for use at first aid stations set up by the rioters, or employees on duty may create disturbances within the facility in support of the rioters’ cause. For example, a wastebasket fire was set in a stairwell in one reported case. Although no real damage resulted, the smoke created confusion and panic among patients and staff. Third, separate treatment areas for rioters and the public may be needed to minimize continuing confrontation.

**External Protection Planning.** Preparations for minimizing damage to the facility and safely moving employees cannot be made at the last minute. Thus, the first step in riot protection planning is to survey the perimeter of the property. For example, this might be the time to recommend fencing the north property line to divert foot traffic from crossing through parking areas. Security administrators should also consider whether exterior lighting is adequately protected to minimize destruction, whether landscaping decorations or other external items should be removed, and how employee vehicles should be protected. The next step is to carefully survey the exterior of the buildings that will require protection. Access doors and windows are of primary concern. Even though normal access points cannot be eliminated during normal operations, administrators must be prepared to quickly authorize restricted access when a riot occurs. The time to make certain that doors are equipped with the proper hardware is before a riot occurs. Security administrators should select the access point that could be controlled best if only one entrance were to be operative. The best entrance is not necessarily the most accessible one. If the facility has an emergency department, two access points are generally required: one for persons seeking medical care and another for everyone else. Windows and other glass areas are primary targets for destruction. Break-resistant glazing material is commonly used for protection. Another method is to precut plywood and install brackets on the window frames to permit easy and quick installation. If no glass protection has been installed or if the protection is minimal, interior blinds or curtains should be closed. If beds are near a window, they should be moved as far from the window as possible. Exterior lighting must be reviewed to determine whether the illumination is adequate. More light is needed during rioting than is needed under normal conditions. Security administrators should also check to determine whether light fixtures can be modified to prevent damage. Generally, little can be done in this regard, but making certain that lights are not within easy reach is at least one step that can be taken.

**Internal Protection Planning.** The interior of the facility should be reviewed to identify critical areas that need additional protection. This additional security may be in the form of hardware, or it may require establishing a security post. Areas of obvious concern are electrical distribution vaults, emergency power areas, equipment rooms (including elevator penthouses), oxygen and medical gas systems, emergency exits, traffic control, and surveillance areas. Organizations should seriously consider placing operators on all elevators. By manually controlling elevators, traffic can be controlled more readily, and in a sense the elevator operators provide an element of security. If emergency security posts are necessary, every possible post location should be given an activation priority so that as emergency conditions develop, the posts can be activated in a logical priority. The protection level will expand and contract during a civil disturbance crisis according to the threat at hand. Fire extinguishers and communications equipment are essential for every post; access lists and special equipment may be needed at particular posts. Planning may indicate that a reasonable approach to providing communications at every post is to install telephone jacks at each location or the use of cellular telephones. Most facilities do not have enough two-way radio equipment available for a significant protection posture; however, this situation is improving with considerable grant money.

A command post is required for all types of emergencies. In larger facilities the central security post is readily adaptable to this function until the emergency incident command post is established. During the emergency, it is suggested that two or three security employees be assigned to a task force that will be immediately available to deploy upon receiving notification from incident command that an emergency response is needed at a specific location.

Small clinics and medical office buildings must take many of the same precautions and plan in the same manner as hospitals do. One advantage of outpatient treatment facilities is that they can be locked up and need not continue to operate. However, past accounts of riot damage have shown that unoccupied buildings receive considerably more damage than occupied buildings.
Pandemic Event

In 2003 a major epidemic of severe acute respiratory syndrome (SARS) infected individuals in 37 countries around the world in a matter of weeks. The SARS event was a near pandemic, but it was effectively controlled before reaching the pandemic state.

Now the H1N1 Influenza A virus (also known as a swine flu virus) is spreading around the world and has been declared a public health emergency of international concern by the World Health Organization. The U.S. Government has also declared the flu outbreak a public health emergency, which is the first step for providing resources and support to the states, including release of stockpiled antiviral medications.7

In terms of security considerations for the HCF, relative to an epidemic and pandemic event, law enforcement and public safety agency support may be available. Unlike other community emergency events, there is no real defined scene that requires emergency response field management by the law enforcement agency. Fire personnel, as part of an EMS response, may, however, tax their resources. The HCF security concerns will be directly related to surge groups and a basic medical treatment concern may be lack of staff.

Security response planning in relation to a pandemic should expect
- A surge of persons seeking medical care that goes well beyond the capability of the facility, resulting in disruptive behaviors, including violence and destruction of property.
- A surge of persons seeking information relative to both inpatients and outpatients.
- A surge of persons (family/relatives) seeking discharge of inpatients who are not patients with a diagnosis of the identified pandemic disease.
- The risk of loss of stockpiled drug supplies via the means of break-ins and violence. An undisclosed off-site security storage site should be considered.

The possibility that such chaos, disorder, and destruction of property will result in the closing of the facility should be part of the EOP.

Active Shooter

While there is a long history of shootings in many facilities, the major shooting events in schools and retail shopping malls have generated serious concern among security practitioners. Hospitals have also been the scene of “active shooters,” killing multiple persons in many incidents, but not in the same high numbers. There have been discussions and meetings concerning security safeguards, preventive measures, and operational security procedures for dealing with such an emergency. There do not seem to be as many answers as there are questions. In most cases, there is little warning that an active shooter event is about to take place.

In most instances of these events, the retrospective players point to early signs of trouble that should have prompted a preventive approach. It is easy to critique after the fact, but difficult to perceive what an individual (or individuals) will do in the future.

Staff Actions

In addition to notifying security and law enforcement, when safe to do so, staff must quickly decide on options such as hiding, evacuation (escaping the scene), or taking action when face to face with the shooter. These options have been advanced for the mall/retail shooting events. They may not be that well suited for patient care staff, who must do all possible to protect the patients as well as themselves.

Communications to Departments and Units. When circumstances permit and the means are available, the best staff action is to seal themselves and patients off by closing and securing doors. This may mean barricading doors with whatever is available (i.e., furniture). In areas where there are no patients, fleeing may be an option if it is perceived safe to do so.

Most active shooter situations are beyond a practical security intervention, and the best course of action may be containment until police arrive.

In order to mitigate an active shooter event, the ability to communicate with departments and patient care units is essential. Forewarning allows for action options to be considered by staff. Overhead paging is a common method of communication with staff and the use of computer alerts is increasing.

It is probably redundant, but the best organizational approach to preventing an active shooter event is to maintain a strong threat policy and procedure along with a strong day-to-day security system.

ACCIDENTAL AND NATURAL EMERGENCY EVENTS

Natural disasters, such as snowstorms, tornadoes, floods, hurricanes, and earthquakes, frequently activate the facility EOP. All of these severe natural phenomena events can significantly affect healthcare operations to varying degrees. The concomitant problems generally involve failure of the electrical system, interruption of deliveries, lack of communications, increased demand for medical treatment, and the isolation of the facility. Fortunately, facilities are not always hit directly by these disastrous weather occurrences, and they can continue to serve the community’s needs with minimal interruption of normal services if proper planning has been completed.

In many cases of severe weather conditions, handling of mass casualties is not required. The focus is on other problems, such as providing housing for employees who cannot leave, finding temporary shelter for people who have been stranded, maintaining supplies such as
food, and transporting essential personnel from their homes to the hospital. When a facility operates under emergency conditions as a result of a community disaster, a unique phenomenon is readily apparent. Everyone pitches in to do practically anything required. The petty jealousies and animosities of the everyday routine quickly disappear. Even student nurses who are normally restricted in day-to-day activities are given more latitude to do the things that need to be done.

In addition to severe weather conditions, there is a host of other events that will put the facility EOP into play. There are ever-increasing events concerning accidents involving hazardous materials that affect scores of people. Transportation accidents occur that require hospitals to provide extreme amounts of minor medical care to high-level trauma care. In terms of transportation accidents, the airplane event often comes to mind; however, of late there have been an increasing number of railroad type accidents. Construction accidents and structure failures are always possible emergency events that force hospitals into an emergency operational mode.

**GENERAL ADMINISTRATIVE AND OPERATIONAL ISSUES**

**Emergency Announcement Codes**

The use of word, number, or color codes to announce an emergency condition to facility staff is virtually common to all hospitals. What is not common is the number of different color codes used and a common matching of a specific color to the type of emergency condition. The exception is the somewhat common codes of Adult Medical Emergency: cardiac arrest (blue), fire (red), and infant abduction (pink).

Numerous hospital organizations have studied the need for a standardized common code system. One of the best known studies, culminating in a comprehensive 81 page report, was that conducted by the Healthcare Association of Southern California in the year 2000.

Another study of emergency codes was conducted by the Colorado Hospital Association. They found a huge mix of different codes by just 59 reporting hospitals. An example of this mix is revealed in the bomb codes reported. There were 13 different codes:

| Code 4   | Code Orange | Dr. Search |
|----------|-------------|------------|
| Code 99  | Code White  | Mr. Search |
| Code Black| Code Yellow | Personnel Alert |
| Code Blue | Dr. Atom    | Code Green |
| Dr. Orange|             |            |

There is little question that standardized codes would result in reduced training time, reduced misunderstandings, and the emergency response would be more efficient. Despite all the efforts of the various groups advocating standardized emergency codes, little progress has been made. One of the obstacles to gaining a consensus is that there appears to be too many different emergency code conditions proposed. The aforementioned California code study recommended 11 different codes, which many healthcare professionals feel is an excessive number of codes. Consensus seems to be that the most practical approach would be to limit the number of standard codes to no more than five codes using color designators. As the debate continues, it is suggested that the three basic codes of blue, red, and pink be used as the basic system of emergency codes with individual facilities adding more codes if they are needed.

When developing a code system, healthcare organizations should not use codes common to other types of organizations, such as Code Amber. Amber Alert is a law enforcement term and should not in any way be confused with a healthcare term that might sound similar.

**Facility Access Control**

In the event of an internal or external emergency, it may be necessary to restrict access for persons entering/leaving the facility as a whole, or a selected area within the facility. The terms _surge_ and _lockdown_ are used frequently when developing the EOP. These two terms are often used without definition and sometimes out of context. The term _surge_ used by a medical caregiver will often be used to refer to a surge of patients. The same term used by the security administrator will generally mean a surge of persons seeking treatment, visitors, curious onlookers, media personnel, and so forth. Likewise, the term _lockdown_ can mean restricting entry, restricting exiting, restricting specific access points (internally or externally), or a combination of such access points.

Electronic Security System Integration, the need to be able to lock down the facility in a very short time, was discussed. The concept of a two-stage lockdown plan was also put forward in the discussion of controlling access during an emergency.

The means to lock down all entrances of all HCFs has become a basic element of healthcare security systems. This important aspect of security has become a national standard practice and will soon become the national standard of care for HCFs treating inpatients and/or outpatients. A recent study revealed that 7% of U.S. hospitals do not have the ability to perform a total lock down of their facilities. It was further reported that it takes another 20% more than 15 minutes to secure entrances and exits.

In a Joint Commission Resources publication, the concept of a three-tiered approach was advanced. Each healthcare organization should decide what emergency access control system will work best for its mission and environment. This decision must then be included in the facility EOP.

Table 42.3 is a snapshot of the various levels of a facility access control system.
Security Staffing Under Emergency Conditions

Perhaps the major challenge for the Security Administrator is staffing. EOPs often call for 8–10 times the number of security officer staffing requirements over the regular day-to-day staffing of the Security Department. In addition, the duration of the emergency can vary from a few hours to days to weeks, requiring expanded security operations. Staffing also depends on the type of emergency. If the emergency is an external transportation accident, staffing will be somewhat easy, as organization staffing will at least be par, and hospital staff willing to stay past their shift or come from home. If it is a pandemic situation, the number of staff on duty may be fewer than normal, due to employee absences, and it is much more difficult to convince off-duty employees that you need them to come into work.

There are several traditional methods of increasing security staff due to an emergency situation, which include preplanned volunteers from other departments and an arrangement with a contract security service if the security department is an in-house program. Neither of these methods works very well. If the emergency involves the community, and if the hospital security program normally relies on any amount of off-duty police coverage, it will be difficult, if not impossible, to satisfy even a minimal amount of expanded security officer man hours.

An agreement with outside security services providers to provide staffing in an emergency would be directly related to the provider’s ability to field such manpower. Again, if the emergency condition is a community emergency, the regular security customers may need extra coverage and the hospital will certainly be in a subordinate position.

An in-house security program that regularly staffs its normal deployment plan with all full-time security officers has a very difficult time maintaining consistent staffing without the use of excessive amounts of overtime. The utilization of a contingent group of part-time officers is a good practice and is helpful when expanded security staffing is needed.

Mutual Aid Resources

Not all emergency planning will be done on a consolidated community-wide basis. Planning for any type of emergency, whether internal or external, requires close liaison with other medical care facilities in the community. The security administrators of healthcare provider organizations should meet regularly for mutual aid planning purposes. An important consideration in mutual aid planning is to join with organizations that are not likely to be involved in the same emergency at the same time. Resources of one facility should be readily available for use in another facility. The planned exchange of resources — whether security officers, vehicles, cameras, and so forth — should be organized, and each organization should sign a formal statement of commitment. These types of documents are often referred to as a memo of understanding.

Security Uniforms and Marked Vehicles

In some assignments or functions, the identification of security personnel is a detriment. Planning should take into account that uniformed authority figures may sometimes create problems. Consideration should be given to certain staff wearing street clothes, that is, drivers who may need to pass through disturbance areas. Drivers should carry a letter indicating that they are employees on official business. Marked vehicles and especially marked security vehicles may also become targets. The objective in using both street clothes and unmarked vehicles is to avoid calling attention to certain security activities.

Employee Travel and Housing

Another problem that requires considerable planning is that employees may not be able to travel freely to and from work because of a curfew, police lines, or fear of harm. Experience reveals that even though employees may be willing to travel to work under adverse conditions, anxious friends or relatives often persuade them to remain at home. Curfew terms vary widely according to local conditions and objectives. A common restriction is to prohibit people under a certain age from being on the streets after a certain hour. When this condition was imposed in a major city, it created a problem for the hospital because many employees were affected. The solution was simple. In addition to their name badge, employees carried a letter addressed to law enforcement officials.
that was signed by the hospital administrator, and contained the employee’s name and address, the time dismissed from work, and a statement that the letter was intended for use only for the date indicated. This approach worked well and was reported to be widely accepted by law enforcement personnel. When police lines are established, altered travel routes are an obvious course of action. When police lines surround the facility, some procedure must be devised for staff access. Staff identification cards or badges are one solution. Another approach may be for a facility representative to be stationed at a central point along the police line to verify employee status. Individuals who attempt to cross the police line can be identified with simple questions about their department, employee number, birth date, or other data. The facility representative will be able to verify many employees by sight. During a civil disturbance, organizations may encourage employees to stay on the premises for their own safety and for the purpose of maintaining adequate staff. Employees sometimes insist on staying regardless of the official stance, and thus some planning for employee housing is mandated. An inventory of beds that can be used in an emergency should be maintained. A thorough review of a facility often uncovers more beds than expected. Beds can sometimes be found in classrooms, blood banks, on-call rooms, and electrocardiogram and electroencephalogram areas. In addition, cots can be set up in many areas for temporary accommodations. To ensure the utilization of all beds and to keep a record of where employees are housed, assignments must be made by a designated facility representative. Employees should not be allowed to assume their own accommodations even in their own departments. When more employees request accommodations than are needed to work, a system of housing authorization by department heads may be necessary to maintain adequate control.

There will of course be additional administrative and operational issues to be defined and addressed by individual healthcare provider organizations.

CONCLUSION

Colling and York, in my opinion, have done a great job in the fifth edition of Hospital and Health Care Security. This chapter, which was written primarily for the healthcare industry, applies to all of us in security management, as the principals and concepts are basically the same. Crisis Management comes in many forms and we must be ready and prepared for it.

Glossary of Terms for Emergency Preparedness*

action plan  See incident action plan.
agency  An agency is a division of government with a specific function, or a nongovernmental organization (e.g., private contractor, business, etc.) that offers a particular kind of assistance. In ICS, agencies are defined as jurisdictional (having statutory responsibility for incident mitigation) or assisting and/or cooperating (providing resources and/or assistance).
all-risk  Any incident or event, natural or human-caused, that warrants action to protect life, property, environment, and public health and safety, and minimize disruption of governmental, social, and economic activities.
area command (unified area command)  An organization established to oversee the management of (1) multiple incidents that are each being handled by an ICS organization or (2) large or multiple incidents to which several incident Management Teams have been assigned. Area command has the responsibility to set overall strategy and priorities, allocate critical resources according to priorities, ensure that incidents are properly managed, and ensure that objectives are met and strategies followed. Area Command becomes Unified Area Command when incidents are multijurisdictional. Area Command may be established at an emergency operations center facility or at some location other than an incident Command Post.
assisting agency  An agency or organization providing personnel, services, or other resources to the agency with direct responsibility for incident management.
chain of command  A series of management positions in order of authority.
command  The act of directing and/or controlling resources by virtue of explicit legal, agency, or delegated authority. May also refer to the Incident Commander.
command post  See incident command post.
command staff  Consists of the Public Information Officer, Safety Officer, and Liaison Officer. They report directly to the Incident Commander. They may have an assistant or assistants, as needed.
communications unit  An organizational unit in the Logistics Section responsible for providing communication services at an incident. A Communications Unit may also be a facility.
emergency management coordinator/ director The individual within each political subdivision that has coordination responsibility for jurisdictional emergency management.

emergency operations centers (EOCs) The physical location at which the coordination of information and resources to support domestic incident management activities normally takes place. An EOC may be a temporary facility or may be located in a more central or permanently established facility, perhaps at a higher level of organization within a jurisdiction. EOCs may be organized by major functional disciplines (e.g., fire, law enforcement, and medical services), by jurisdiction (e.g., federal, state, regional, county, city, tribal), or some combination thereof.

emergency operations plan (EOP) The plan that each jurisdiction has and maintains for responding to appropriate hazards.

event A planned, nonemergency activity. ICS can be used as the management system for a wide range of events, e.g., parades, concerts, or sporting events.

facilities unit Functional Unit within the Support Branch of the Logistics Section that provides fixed facilities for the incident. These facilities may include the Incident Base, feeding areas, sleeping areas, sanitary facilities, and so forth.

incident An occurrence or event, natural or human-caused, that requires an emergency response to protect life or property. Incidents can, for example, include major disaster emergencies, terrorist attacks, terrorist threats, wildland and urban fires, floods, hazardous materials spills, nuclear accidents, aircraft accidents, earthquakes, hurricanes, tornadoes, tropical storms, war-related disasters, public health and medical emergencies, and other occurrences requiring an emergency response.

incident action plan (IAP) An oral or written plan containing general objectives reflecting the overall strategy for managing an incident. It may include the identification of operational resources and assignments. It may also include attachments that provide direction and important information for management of the incident during one or more operational periods.

incident base Location at the incident where the primary logistics functions are coordinated and administered. (Incident name or other designator will be added to the term Base). The Incident Command Post may be collocated with the Base. There is only one Base per incident.

incident command post (ICP) The field location at which the primary tactical-level, on-scene incident command functions is performed. The ICP may be collocated with the incident base or other incident facilities and is normally identified by a green rotating or flashing light.

incident command system (ICS) A standardized on-scene emergency management construct specifically designed to provide for the adoption of an integrated organizational structure that reflects the complexity and demands of single or multiple incidents without being hindered by jurisdictional boundaries. ICS is the combination of facilities, equipment, personnel, procedures, and communications operating within a common organizational structure, designed to aid in the management of resources during incidents. It is used for all kinds of emergencies and is applicable to small as well as large and complex incidents. ICS is used by various jurisdictions and functional agencies, both public and private, to organize field-level incident management operations.

incident commander (IC) The individual responsible for all incident activities, including the development of strategies and tactics and the ordering and the release of resources. The IC has overall authority and responsibility for conducting incident operations and is responsible for the management of all incident operations at the incident site.

incident objectives Statements of guidance and direction necessary for the selection of appropriate strategy(ies) and the tactical direction of resources. Incident objectives are based on realistic expectations of what can be accomplished when all allocated resources have been effectively deployed. Incident objectives must be achievable and measurable, yet flexible enough to allow for strategic and tactical alternatives.

jurisdiction A range or sphere of authority. Public agencies have jurisdiction at an incident related to their legal responsibilities and authority. Jurisdictional authority at an incident can be political or geographical (e.g., city, county, tribal, state, or federal boundary lines) or functional (e.g., law enforcement, public health).
management by objective  A management approach that involves a four-step process for achieving the incident goal. The management by objectives approach includes the following: establishing overarching objectives; developing and issuing assignments, plans, procedures, and protocols; establishing specific, measurable objectives for various incident management functional activities and directing efforts to fulfill them, in support of defined strategic objectives; and documenting results to measure performance and facilitate corrective action.

mitigation  The activities designed to reduce or eliminate risks to persons or property or to lessen the actual or potential effects or consequences of an incident. Mitigation measures may be implemented prior to, during, or after an incident, and they are often formed by lessons learned from prior incidents. Mitigation involves ongoing actions to reduce exposure to, probability of, or potential loss from hazards. Measures may include zoning and building codes, floodplain buyouts, and analysis of hazard-related data to determine where it is safe to build or locate temporary facilities. Mitigation can include efforts to educate governments, businesses, and the public on measures they can take to reduce loss and injury.

multiagency coordination systems (MACS)  Multiagency coordination systems provide the architecture to support coordination for incident prioritization, critical resource allocation, communications systems integration, and information coordination. The components of multiagency coordination systems include facilities, equipment, emergency operations centers (EOCs), specific multiagency coordination entities, personnel, procedures, and communications. These systems assist agencies and organizations to fully integrate the subsystems of the NIMS.

preparedness  The range of deliberate, critical tasks and activities necessary to build, sustain, and improve the operational capability to prevent, protect against, respond to, and recover from domestic incidents. Preparedness is a continuous process. Preparedness involves efforts at all levels of government and between government and private-sector and nongovernmental organizations to identify threats, determine vulnerabilities, and identify required resources. Within the NIMS, preparedness is operationally focused on establishing guidelines, protocols, and standards for planning, training and exercises, personnel qualification and certification, equipment certification, and publication management.

preparedness organizations  The groups that provide interagency coordination for domestic incident management activities in a nonemergency context. Preparedness organizations can include all agencies with a role in incident management, for prevention, preparedness, response, or recovery activities. They represent a wide variety of committees, planning groups, and other organizations that meet and coordinate to ensure the proper level of planning, training, equipping, and other preparedness requirements within a jurisdiction or area.

prevention  Actions to avoid an incident or to intervene to stop an incident from occurring. Prevention involves actions to protect lives and property. It involves applying intelligence and other information to a range of activities that may include such countermeasures as deterrence operations; heightened inspections; improved surveillance and security operations; investigations to determine the full nature and source of the threat; public health and agricultural surveillance and testing processes; immunizations, isolation, or quarantine; and, as appropriate, specific law enforcement operations aimed at deterring, preemting, interfering, or disrupting illegal activity and apprehending potential perpetrators and bringing them to justice.

recovery  The development, coordination, and execution of service- and site-restoration plans; the reconstitution of government operations and services; individual, private-sector, nongovernmental, and public-assistance programs to provide housing and to promote restoration; long-term care and treatment of affected persons; additional measures for social, political, environmental, and economic restoration; evaluation of the incident to identify lessons learned; post incident reporting; and development of initiatives to mitigate the effects of future incidents.

span of control  The number of individuals a supervisor is responsible for, usually expressed as the ratio of supervisors to individuals. (Under the NIMS, an appropriate span of control is between 1:3 and 1:7.)

unity of command  The concept by which each person within an organization reports to one and only one designated person. The purpose of unity of command is to ensure unity of effort under one responsible commander for every objective.
REFERENCES

[1] Blair JD. Are medical facilities doing enough to prepare for catastrophic events? Healthcare Construction & Operations; 2008;11.

[2] Weronik R. Securing our hospitals: GE Security and IAHSS healthcare benchmarking study. Presented at International Association for Healthcare Security and Safety Mid-Winter Meeting and Seminar; January 21, 2008.

[3] University of Wisconsin hospital completes largest mass casualty drill in state history. Emergency Management Alert; 2009. HCPRO, 8 (25).

[4] Hsu S, Tyson AS. Pentagon to detail troops to bolster domestic security. Washington Post; 2008.

[5] A new breed of threat. Access Control and Security Systems; 2004:55. (Note: best information provided.)

[6] Hall MDC. Hospital installs radiation detectors. USA Today; 2008:19A.

[7] The H1N1 influenza a virus: A test case for a global response. Rapid public health response project. Washington DC: The George Washington University School of Public Health and Health Services; 2008. Washington DC. 1.

[8] Colorado Hospital Association. Emergency code use in Colorado: Results from a survey of Colorado hospitals. Retrieved June 25, 2009, from <http://www.cha.com/index.php?option=com_content&task=view&id=959&Itemid=208>.

[9] 1 in 4 hospitals face lock-down challenges. Campus Safety Magazine. Retrieved July 24, 2009, from <http://www.campussafetymagazine.com/News/Default.aspx?NewsID=3171>.

[10] Colling R. Security issues for today’s health care organization. Oakbrook Terrace, IL: Joint Commission Resources; 2002.