The Joint Commission clarifies its generator testing requirements
Tests may be combined in certain situations

As of July 1, to be in compliance with EC 7.40, hospitals needed to have completed a four-hour generator test at some point within the past 36 months—and perform a similar generator run every 36 months thereafter.

This testing approach follows the National Fire Protection Association's (NFPA) standard NFPA 110, Emergency and Standby Power Systems.

Generator testing is a big deal these days: In interviews with Briefings on Hospital Safety, recently surveyed hospital safety managers nationwide say that Joint Commission representatives requested to see generator testing records. That’s not a surprise to David Stymiest, PE, CHFM, FASHE, a senior consultant for Smith Seckman Reid, Inc., based in Nashville.

Stymiest says he has heard that surveyors have zero leeway on that count, as they’ve been instructed to check generator testing wherever they go.

Two bomb scares offer this hospital a chance to upgrade its planning

Imagine how disconcerting it would be to find a half-finished pipe bomb abandoned on your hospital’s loading dock. Now suppose that a couple of weeks later, police suddenly cordon off the streets around the facility because they’ve found two more devices—this time, wired and ready to blow—around the perimeter of the building.

You might wonder how your staff members would react and whether your emergency response plan would rise to the occasion.

San Francisco General Hospital (SFGH) learned firsthand how its disaster plan would stack up, as the above-mentioned scenarios unfolded May 22 and June 6 at an outpatient clinic on its sprawling urban campus. Eventually, police explosives experts rendered the second round of devices inert, and everyone went home safe.

Let incidents reshape your plan
Taking the initiative, emergency planners at SFGH integrated the lessons they learned into their response plan.
“So a surveyed facility can be pretty sure [it] will have to produce generator test records,” says Stymiest, who is chairperson of NFPA 110’s Technical Committee on Emergency Power Supplies.

Most hospitals that Stymiest talks to satisfy the test requirement via a load bank (see “Tech talk: Details about load banks and 30% nameplate” on p. 4 for more). However, some hospitals have used what is called a “dynamic load”—switching the emergency loads over to a generator and performing a test to verify that the system does indeed power its emergency loads.

**What tests meet which requirements?**
Besides the four-hour test, EC.7.40 also requires the following:

- Generator tests 12 times per year for 30 minutes that draw at least 30% nameplate, or energy capacity, of the equipment (if a generator doesn’t hit 30%, the hospital may substitute a supplemental test at various nameplate ratings totaling two hours, as outlined in EC.7.40)
- Automatic transfer switch tests 12 times per year

The question that hospitals had after going through the four-hour test: Does that generator run also satisfy the requirement for monthly 30-minute tests, as well as the potential annual, two-hour generator tests?

Before 2007, the answer was no. After The Joint Commission published a clarification in its July Environment of Care News, the answer is yes, provided that for the duration of the four-hour test, it draws at least 30% nameplate.

This option applies only if you’re running diesel engines; other types of generators have no 30% requirement.

**Actual incidents can count as tests**
Further, if an actual power outage occurs that lasts for at least four hours (and draws at least 30% nameplate for diesel generators), that counts for the required four-hour test and for whatever shorter tests that might be eligible, The Joint Commission says.

For example, if it’s been more than 20 days since your last half-hour test, an outage lasting five hours that draws enough power would satisfy requirements for monthly, annual, and triennial tests.

But if you’re doing a four-hour load bank that draws enough power, it satisfies only the two- and four-hour requirements, because the monthly testing requirements also include transferring the facility’s power over to generators to confirm that the transfer switches still work.

Other events can substitute as tests, too, The Joint Commission says in its clarification. Hospitals running their emergency power supply systems for four hours as part of a peak-shaving agreement with a local utility may also satisfy the triennial test requirement, provided they meet all of the other provisions of EC.7.40.

**Hospitals ask for clarification**
If all this sounds confusing, you’re not alone, says

---

**Elements of emergency power testing programs**
The new provisions of EC.7.40 should prompt hospitals to review and reevaluate their current emergency power plans. The following are three elements important to every emergency power system management plan:

1. **Emergency power gap analysis**—Figure out where you need power most critically during outages of several different severities and how to get that power to those critical areas

2. **Emergency power vulnerability analysis**—Determine the weak spots of your generators

3. **Risk management plan**—Take those identified vulnerabilities and come up with solutions or mitigations for them

Source: David Stymiest, PE, CHFM, FASHE, senior consultant for Smith Seckman Reid, Inc., based in Nashville.
Dan Chisholm, emergency power supply systems consultant for the Motor and Generator Institute of Winter Park, FL. Chisholm is also a member of the NFPA 110 technical committee.

The Joint Commission initially required separate two- and four-hour tests. After hospitals expressed their discontent, The Joint Commission and American Society for Healthcare Engineering (ASHE) polled the NFPA technical committee about a formal interpretation of NFPA 110. Combining tests is fine with committee members, as long as the requirements for each are similar.

“Overwhelmingly, we voted to tell [The Joint Commission] that one test would be sufficient,” Chisholm says.

Because of the way that ASHE and The Joint Commission worded the question, the NFPA could not issue a formal interpretation of the standard, he explains.

However, the technical committee’s stance was clear enough to The Joint Commission that it issued the clarification, with the caveat that future NFPA action could alter the situation.

The NFPA technical committee is expected to streamline the next edition of the standard, scheduled for 2009 release, says Chisholm. He hopes that The Joint Commission and the Centers for Medicare & Medicaid Services will follow the new standard as written, without additional rulemaking.

“We hope to simplify it so that it will be easy for anyone to understand and won’t be so dadgum convoluted,” Chisholm says.

Generator records need to be in order
Surveyors look for a few basic items in your generator testing documentation:

- That the hospital conducted the testing
- That testing lasted for the prescribed interval
- That the load bank or actual loads from the facility drew enough to satisfy the 30% requirement for diesel generators
- That the hospital operated transfer switches properly

However, there are more actions that a hospital can take to move beyond the basics and show The Joint Commission that the facility has developed a sound emergency power management plan.

In September, 2006, The Joint Commission issued a Sentinel Event Alert that outlined preventive steps to help avoid problems caused by power disruptions.

The Alert discussed a number of testing measures that The Joint Commission recommends hospitals carry out, and offered examples of clinical contingency plans that hospitals could put into place during a power loss.

Examples included:

- Accessing drugs marooned in automated dispensing machines
- Using two-way radios in a facility as communication backup
- Maintaining communications with hospital leaders who are off-site

Safety managers who read that Alert might find clues to what surveyors look for, Stymiest says. The big points are to address any problems that generator testing reveals and put detailed thought into handling realistic power outage scenarios—including those caused internally by equipment failures and externally, such as by weather conditions.

“It’s asking the organization to go a little bit further and look beyond just the numbers,” Stymiest says of the Alert. “Make sure the lessons learned from whatever happened during the testing are investigated and followed through . . . to improve the reliability of the overall power system.”

“We hope to simplify [NFPA 110] so that it will be easy for anyone to understand and won’t be so dadgum convoluted.”

—Dan Chisholm
Generator testing

In his ASHE monograph, Managing Hospital Emergency Power Systems: Testing, Operation and Maintenance, Stymiest points out that during monthly testing, emergency power systems can fail and transfer switches might break. It is better for testing to uncover those problems than to find out during an emergency, he writes. The monograph, available for free on ASHE’s Web site (www.ashe.org), is well worth reading.

Tech talk: Details about load banks and 30% nameplate

Hospital safety managers and facility directors might wonder why The Joint Commission is keen on running generators at a minimum of 30% capacity during load bank or real-world testing.

That mantra actually comes from generator manufacturers, who know diesel engines and the way they run, says Dan Chisholm, emergency power supply systems consultant for the Motor and Generator Institute of Winter Park, FL.

“If you can’t run your diesel engines at least 30%, you’re going to cause engine damage,” Chisholm says.

That’s because at lower levels of output, unburned fuel accumulates in the engine, a condition called “wet stacking.” At 30% capacity or higher, the inside of the engine gets hot enough to burn all the fuel piped through it.

The 30% rule also relates to another concept that might confuse hospital safety managers new to the technical side of emergency power: using a load bank versus the actual hospital power load for generator testing.

Some people might assume that a hospital would bring in a load bank—basically, a power-eating device on a trailer in the parking lot—because it’s easier than arguing with clinicians and administrators about what would be the best time to test the generators.

That’s not true, though, Chisholm says. The reason most facilities use a load bank is that regular power loads at a hospital won’t necessarily tax the emergency system enough to satisfy the 30% rule.

There are ways to complete the test without a load bank, says Dave Stymiest, PE, CHFM, FASHE, a senior consultant for Smith Seckman Reid, Inc., based in Nashville.

For example, hospitals that want to skip the load bank may try to switch the facility over to generator power at night or on weekends.

That can be problematic because there’s not enough bustle during the off hours to draw that 30% and give generators the realistic workout that they’d get when, for example, the ORs are in use, Stymiest says.

Hospitals may be able get around that issue by turning on lights and similar equipment in empty ORs to simulate the power load of actual procedures.

Some facilities will try generator testing during peak hours just to see if the emergency power supply system can sustain the rigors of a blackout.

But Stymiest is “not a big fan” of this approach, he says. Imagine the risk of switching a surgical suite to faulty generator power in the midst of a patient procedure.

“I think a better idea is to minimize the chance of something going wrong and adversely affecting patient safety,” Stymiest says. Hospitals can test generators during periods of low clinical activity as long as they realize that the stress on the generators will be less than during peak periods, he says.
Your new resource: The Hospital Safety Center

We here at HCPro are excited to announce the debut of a comprehensive resource that we hope all of you will check out: the Hospital Safety Center. Available online at www.hospitalsafetycenter.com, this Web site is jam-packed with regulatory analysis, sample forms, and risk assessment tools.

As Briefings on Hospital Safety subscribers, all of you will become regular members of the Hospital Safety Center at no extra charge.

At this level, you will be able to enjoy the following added benefits to your subscription:
- A new feature called “Mac’s Safety Space,” in which our resident safety consultant, Steven MacArthur, will give field advice and help with survey concerns
- For the first time, searchable archives of our popular “Safety Talk” online forum
- A special report archive that currently has nine reports available for downloading

As an upgrade, you can also sign up for our platinum membership, which centers on these new features:
- An in-depth regulatory compliance database that you can browse or search by regulator
- More than 100 sample forms and policies
- Access to electronic workstations for hazard vulnerability analyses, infection control risk assessments, and interim life safety measures

By the way, those of you who subscribe to Briefings on Hospital Safety’s Regulatory Compliance Manual will automatically become platinum members.

We’re in the process of notifying all of you about your new login information. If you haven’t heard from us but want to get onto the Web site right away, please call our customer service center at 800/650-6757.

So please log onto www.hospitalsafetycenter.com and explore this added subscriber benefit, which will become the new face of our hospital safety community.
**Bomb scares**  <p. 1

“We did a report that looked at what worked well [and] what didn’t go so well,” says Delvecchio Finley, SFGH’s administrator for support services. “You learn to check your assumptions in the aftermath of an event. We have already implemented changes.”

The bomb incidents forced SFGH to look hard at its emergency plan and update pieces of it, such as employee notification procedures, he says. (See “Employees found out about the bomb scare through TV news” on p. 7.)

In the future, the hospital will also pay more attention to closing times of buildings and what to do if an incident unfolds during off-hours. Previous iterations of the emergency plan put more emphasis on threats to the main hospital, Finley says. SFGH will more heavily involve satellite buildings in upcoming drills.

Police believe a 16-year-old boy planted the three pipe bombs outside the building, although at press-time authorities continued to work on the case, says investigator Jeff Lindberg of the San Francisco Police Department.

**Use drills to promote calm responses**

Defusing explosives might be the purview of the police, but safety managers can help diffuse tensions in the difficult scenario of a bomb scare.

Emergency plan tests that simulate a bomb scare can make the real deal less scary for staff members. However, having gone through an actual scare, no amount of practice can completely prepare employees for the real thing, Finley adds.

Nonetheless, having an action plan in place can help and will likely receive a nod from regulators. That plan should cover the following:

- Defining a suspicious package
- What steps to take once someone identifies a suspicious package
- Evacuation procedures (e.g., who orders the evacuation, when it occurs, and which people evacuate)
- Giving cheat sheets to everyone involved so that they know what steps to take when a tense situation unfolds

**Shift directions during a drill**

Here’s an important step to think about: Change instructions to staff members during a drill, says Finley.

That advice might sound strange at first. But during a bomb scare, authorities may ask people to do different things or move to alternative places several times as police learn more details about the device and the threat it poses.

“As you become more informed about what you’re dealing with, your instructions become more evolved,” Finley says. “You might be telling one group of staff one thing, and then something different an hour later. That can appear disorganized or chaotic . . . It’s really important to [drill it] to command the confidence in them so that they will follow instructions.”

Also, ensure that everyone takes an evacuation seriously, whether it’s a drill or real—including administrators, Lindberg says. “I’m sure you have special people in the hospital environment who

**Offer training in the mail room**

Your hospital’s mail room can be a gateway for suspicious devices. Packages that a hospital receives with lots of tape, no return addresses, grease marks, leaks, or excessive postage should raise suspicions, says investigator Jeff Lindberg of the San Francisco Police Department.

Mail workers who regularly handle packages will probably be able to spot the suspicious ones on their own. But to help them further, many local law enforcement authorities publish brochures or offer other training, Lindberg adds. Make that training part of your emergency plan.
think they’re special and immune to certain issues,”
such as participating in drills, he says. “But it’s really
important that your administrators fully endorse and
back up your safety plan . . . If it goes to the top, it
builds viability and credibility [for your plan] if an
incident actually occurs.”

Learn the nature of a dubious device
Suspicious packages show up in hospitals and other
public spaces on a daily basis. Police in Washington,
DC, alone received 1,014 calls reporting them during
2006, or three per day, according to an Associated
Press story published on July 16.

The key to spotting suspicious packages involves the
common sense of people working in the hospital. For
example, staff members who routinely treat homeless
people might be used to seeing odd boxes of things—
or even shopping carts full of possessions—in wait-
ing rooms, Finley says. The same boxes might cause
alarm at other hospitals.

Police in San Francisco take staff members with them
when looking for bombs or other devices, because
someone who works at a site can more readily spot
things that don’t seem to fit in, Lindberg says.

How do you know a suspicious device when you see
one? First, there are obvious signs that leave no doubt,
such as a metal or PVC pipe with two end caps and
a wick coming out of it or an item taped up with a
timer, Lindberg says.

Next, an abandoned box, suitcase, or briefcase might
draw suspicion in certain contexts, such as when
someone leaves it in the entrance of an area where
controversial research is underway—especially if a
facility received prior threats.

“It doesn’t take a stretch to make the determination
that you may have a suspicious device or certainly a
device that warrants increased scrutiny” in such cases,
Lindberg says.

Employees found out about the bomb scare through TV news
San Francisco General Hospital (SFGH) is rethink-
ing some elements of its communications strategies
with the media since two pipe bomb incidents in
May and June.

On one hand, the incidents were minor and
police rendered the bombs safe before anyone
got hurt. The scares took place at an outlying
campus clinic, away from the main hospital. On
the other hand, once police cordoned off a local
street, television media came to the scene and
captured live video. Some staff members heading
out for a shift change learned about the unfolding
potential crisis through TV reports and not via in-
house channels.

The hospital’s response organizers chose to target
their internal communications by notifying people
in the clinic and another building where occupants’
safety was potentially at risk. They did not real-
ize until later how many more employees became
aware of what happened through TV.

Hospital plans will evolve
The timing of these incidents in regards to shift
changes and other sticky issues will be taken into
account should an incident like this happen again,
says Delvecchio Finley, SFGH’s administrator for
support services.

The hospital’s action plan worked well, but officials
need to further develop their staff notification and
external communications plan based on how the
incidents unfolded, he says.

Police, sheriff, and hospital authorities met in a rou-
tine debriefings to break down the events and ana-
lyze what went well and what needed improvement.

“Our practice is to use the media as a partner,”
Finley says. “Once they arrive, it’s incumbent upon
you to not take an antagonistic view and say,
‘They’re here, let’s keep everything from them’ . . .
They’re also part of the system the public relies on
for information, so we all have to work together.”
ASHE conference coverage

Prepare now for SOC and emergency plan changes

With a full switchover to the electronic Statement of Conditions (SOC) coming on September 1 and new emergency management rules taking effect four months later, the last third of 2007 looks to be a busy one for accredited hospitals.

In fact, Joint Commission changes led the discussions at several sessions of the American Society for Healthcare Engineering’s (ASHE) annual conference in New Orleans in July.

The following is an overview of the important highlights to stay on top of.

PFI import tool finally debuts
As of September 1, all outstanding plans for improvement (PFI) must be entered electronically through The Joint Commission’s extranet. That mandate includes PFIs that you may have on paper or in your own Excel spreadsheets.

Hospitals that don’t meet this deadline will likely bring unwanted attention on themselves. If you have PFIs that aren’t in the e-SOC but will be completed before September 1, you don’t need to import them.

To help with the conversions of existing PFIs, the commission released its long-awaited import tool on July 9 at the ASHE conference. The program asks you to configure your Excel file as a csv (comma-separated value) file before importing it into The Joint Commission’s system.

“It’s basically taking your fancy Excel file and crunching it down to a very simplistic format,” said George Mills, FASHE, CEM, CHFM, senior engineer at The Joint Commission. Mills spoke during the ASHE conference.

Automated e-mail responses from the commission will let you know whether your import was successful and whether errors in the file require corrections.

A user group made up of people with varying levels of Excel experience previously tested the import tool. “As cumbersome as this seems, it was pretty easy for [testers] to do,” Mills said. For example, everyone in the group got at least 400 PFIs transferred into the e-SOC within two hours, he added. (See “Tips on to use the new e-PFI import tool” below.)

Emergency operations plans evolve
On January 1, far-reaching revisions to EC.4.10 (developing emergency management plans) take effect. The August Briefings on Hospital Safety detailed the specific changes.

“The Joint Commission is very serious about emergency readiness,” Mills said.

Tips to use the new PFI import tool

Follow the advice below to help you use The Joint Commission’s new import tool for Excel-based plans for improvement (PFI):

✓ To avoid errors, make sure the number of columns in your Excel spreadsheets match those in the import tool (including column widths).
✓ Accredited hospitals can read click-by-click instructions for the PFI tool on The Joint Commission’s extranet site and also view a sample. The key is to follow those directions closely when transferring your PFIs.
✓ Use the online sample PFI to practice your imports ahead of time and then delete it from your (SOC) account when you’re done.
✓ Choose the “save as” option for the sample PFI and cut and paste entries from your Excel spreadsheet into the import tool.
✓ Don’t put a dollar sign into your projected cost entries, as the symbol will create errors in the program.

Source: George Mills, FASHE, CEM, CHFM, senior engineer at The Joint Commission.
One term to become familiar with is the “emergency operations plan,” which, in broad terms, replaces the traditional emergency management plan requirements, says Susan McLaughlin, MBA, SASHE, president of SBM Consulting, Ltd., in Barrington, IL. McLaughlin also spoke during the ASHE conference.

The old emergency management plan provided a summary of actions that hospitals would undertake under their emergency operations plans.

One of the revisions comes under the new EC.4.11 (managing the consequences of emergencies), as the standard requires hospitals to communicate their vulnerabilities to response agencies and identify the capabilities of the community to meet hospital needs.

This requirement was borne out of The Joint Commission’s frustration with medical centers’ lack of planning with their communities, Mills said.

As always, paperwork is vital

To document this communication with the community, create a summary for surveyors that includes the following items as outlined by Mills:

- Minutes of meetings with community agencies
- Identified areas of improvement
- A punch list of actions you’ll undertake
- If necessary, a written account of being unable to meet with the community

All of the above items count as evidence that the hospital has taken action under EC.4.11, Mills said. One way to spark this communication is to ask your hospital’s CEO to contact the mayor or town manager of your community, he added.

A 96-hour survival period

Another important change will be in EC.4.12 (developing an emergency operations plan), which mandates that the plan identifies the hospital’s ability to survive on its own for 96 hours without help in several critical areas.

In earlier drafts, this requirement stated 72 hours instead of 96, but The Joint Commission decided that period wasn’t long enough in light of what happened to Gulf Coast facilities after Hurricane Katrina in 2005, Mills said.

Lasting for 96 hours without assistance may be a tough goal for some hospitals because of limited storage space and just-in-time supplies, McLaughlin said.

“Realistically analyze what you can do and the limitations of what you can do,” she said.

Evacuating the hospital before 96 hours has elapsed is an acceptable option to list in emergency operations plans, Mills said.

New twist affects emergency tests

A change under EC.4.20 (testing emergency plans) mandates at least one annual emergency management exercise that includes a scenario that escalates to the point at which the local community can no longer help the hospital.

This escalation aspect can be part of your two regular yearly disaster drills, Mills said.

Further, you can conduct the community portion of the test as a tabletop exercise if local authorities can’t participate in the drill, he added.

Debate continues over new emphasis

There is a movement within The Joint Commission to create a new chapter in the accreditation manual for the emergency management standards, starting in 2009, Mills said.

“My personal opinion is that it makes sense to extract it out as a separate chapter,” because it would draw more attention to the requirements from hospital administrators and nursing directors, he said.

If that shift in chapters occurs, it won’t necessarily indicate any new requirements, McLaughlin said.
Bits & briefs

Congressional committee nixes fit-test exemption
Three years of tuberculosis (TB) fit-testing immunity for hospitals might end with the next federal fiscal year, which begins October 1.

The 2008 appropriations bill for the departments of Health and Human Services, Labor, and Education passed out of the House Appropriations Committee without the TB fit-testing amendment. The amendment currently prohibits OSHA from citing employers for not conducting annual fit-testing for workers who wear respirators to protect themselves from TB.

The committee failed to approve the prohibition amendment by a 27–38 vote, reported the American Hospital Association's News Now on July 11. The association has long supported the annual fit-testing exemption because it is labor-intensive, expensive, and “of unproven benefit for preventing exposure to TB,” according to the article.

However, the full Congress could reinstate the measure.

Annual fit-testing for tight-fitting respirators is a requirement of OSHA’s respiratory protection standard (1910.134). The recent OSHA recommendations for protection against pandemic and avian influenza referenced the need for fit-testing in compliance with the standard. Now the same will apply for respirators worn to prevent TB exposure.

Patient charged with alleged arson in hospital fire
Rhode Island state police planned to file first-degree arson charges against a patient in the adult psychiatric ward at Eleanor Slater Hospital in Cranston, RI, according to The Providence Journal.

The patient allegedly set his mattress on fire and caused the evacuation of 95 patients and 40 staff members at the three-story facility on July 10, police told the Journal. Firefighters quickly extinguished the blaze, and no one suffered injuries.

The fire was the third of the day on the property; two electrical fires knocked out phone and Internet service for several buildings on the hospital campus.

The patient escaped during the evacuation, but police caught up to him on a nearby highway as he was allegedly in possession of tissues and a lighter. The patient had been combative before the fire broke out, hospital sources told the newspaper.

ASHE outlines hand foam allowances
Here are further details about the International Code Council’s (ICC) approval of alcohol-based hand foam dispensers in exit corridors.

The ICC’s approval will become part of its International Fire Code (IFC). According to a bulletin from the American Society for Healthcare Engineering (ASHE), the revision limits the use of hand foam to:
- Level 1 aerosol dispensers with a maximum volume of 18 oz (Level 1 refers to combustible aerosols)
- 10-gal maximum of liquid hand gel or aerosol foam in a corridor per smoke compartment

The IFC classifies aerosols under three levels based on the heat given off when they burn, with Level 1 giving off the least heat and Level 3 giving off the most heat.

ASHE recommends that facility directors share the news of the ICC’s decision with infection control professionals, safety committees, and community fire officials. To read the full ASHE bulletin, go to www.ashe.org/ashe/codes/handrub/index.html.

A small spill creates bigger problems
Four ounces of phenol—a chemical used to remove warts—isn’t enough to be toxic, hospital officials in Pittsburgh said after a pharmacy spill on June 25.

But just the same, the strong smell of the chemical set off a small evacuation of the University of Pittsburgh Medical Center South Side’s pharmacy department, according to KDKA-TV.

After hospital employees cleaned up much of the spill, a hazardous materials team performed a secondary cleanup and ventilated the area in the hospital where
fumes persisted, which precipitated moving a few patients, KDKA reported.

The CDC publishes revised isolation precautions
The Centers for Disease Control and Prevention (CDC) finally released a long-awaited set of guidelines in June that updates and expands its isolation precautions.


This is the CDC’s first major revision to the guidelines, which it first released for hospitals in 1996.

One of the big changes is that these new guidelines now apply beyond hospitals to include settings such as ambulatory care, long-term care, home care and infusion services, as well as special environments such as pediatric wards, ICUs, and burn units.

Chiller pipe rupture causes a hospital scare
A Freon leak created a scare in a building under construction at Cottage Hospital in Santa Barbara, CA.

The gas leaked from a chiller pipe, which triggered a hazardous materials alarm in the larger facility, according to KSBY-TV. Fire department hazmat teams responded to the alarm.

After suiting up in full respiratory gear, firefighters tracked the leak to the basement of the building under construction, and they found that construction workers sheared an active Freon chiller pipe. Within two hours, authorities had ventilated the building and cleaned up the leak.

Fire leads to evacuation in a nearby hospital
A fire that started in a dentist’s office in Macon, GA, caused a nearby hospital to evacuate about 30 patients and several more staff members on July 9.

As a precaution, caregivers at the Children’s Health Center at The Medical Center of Central Georgia relocated patients to other buildings and outside, according to the Macon Telegraph.

The fire ignited in the basement of the dentist’s office, where gas cans, nitrous oxide and oxygen cylinders, and paper started burning, the Telegraph reported. It wasn’t clear what started the fire.

Review your security policies for prisoner patients
After an inmate undergoing an MRI procedure wrestled a gun from a corrections officer and allegedly shot him dead on June 25 at the University of Utah Medical Center in Salt Lake City, the hospital instituted several new rules regarding treatment of forensic patients.

According to the medical center:
- All state Department of Corrections inmates brought to a University Health Care facility will be escorted by two officers. All inmates will wear wrist and ankle restraints.
- Inmates brought to University Health Care facilities from the county jail will have either one or two officers, depending on the risk the inmate represents. All jail inmates will wear wrist and ankle restraints.
- Officers will give care providers a summary of inmate history and risk potential before an inmate receives care.
- Clinicians will defer to corrections and jail officers about whether it is appropriate to remove any restraints in the course of treatment. If an agreement can’t be reached about the removal of restraints, the inmate will not receive care at that time.
- Healthcare workers won’t request that inmates have restraints removed for any reason other than what is needed in the course of a physical exam or procedure. Under no circumstances should an inmate be removed from restraints to complete paperwork or sign a document.
- When feasible, clinicians will use a telemedicine network to treat inmates.
Estimating that fewer than half of healthcare professionals receive influenza vaccinations, the Centers for Disease Control and Prevention (CDC) wants hospitals to improve vaccination coverage among their workers. In its latest recommendations for the upcoming flu season, the CDC suggests that hospitals consider vaccination rates among workers to be a measure in patient safety quality programs. The CDC also encourages medical centers to seek signed declination statements from workers who decline the inoculation.

Healthcare workers who should receive yearly flu shots include the following:

- Physicians
- Nurses
- Employees of nursing homes and chronic-care facilities who have contact with patients or residents
- Students in these professions who will have contact with patients
- Medical emergency response workers
- Workers in both hospital and outpatient care settings

Although the CDC recommendations aren’t mandatory, The Joint Commission supports them. On January 1, infection control (IC) standard IC.4.15 went into effect, requiring hospitals to offer flu vaccines to all staff members, including volunteers and licensed independent practitioners. IC.4.15 also requires facilities to determine why staff members refuse flu shots and then work to overcome these obstacles. Hospitals should verify the status of employee flu vaccination programs and determine whether there are adequate resources to improve vaccination rates among healthcare workers.

To read the full CDC recommendations, formally called Prevention and Control of Influenza: Recommendations of the Advisory Committee on Immunization Practices, go to www.cdc.gov/flu/professionals/vaccination.
The most basic activities that hospital security directors and their officers perform help protect hospitals against lawsuits, said Norman D. Bates, Esq., president and founder of Liability Consultants, Inc., in Boston.

By assessing security risks and responding, hospital security programs help maintain safe facilities and protect patients, visitors, and staff members. And by knowing the reasons commonly behind lawsuits, security directors can learn from the experiences and mistakes of others who have been sued for inadequate security measures, and develop more effective programs themselves, said Bates, who spoke during the International Association for Healthcare Security and Safety annual meeting in Boston in June.

Although hospitals cannot prevent all crime, the basic rule is that property owners are required to maintain reasonably safe premises in light of the risk of crime, Bates said.

Going to court and having to defend your hospital’s security program is an unenviable task. A court case that alleges inadequate security will put your security program under a microscope, Bates said. “It’s an exhaustive, exposing, humiliating process,” he added.

Judgments in liability cases generally cost facilities in the $500,000-$600,000 range, Bates said.

The following, he said, are the top 10 reasons for lawsuits involving premises security, and how hospitals can avoid them:

1. Failure to assess and respond to risks
   Be sure your security program meets the needs of your security will put your security program under a microscope, Bates said. “It’s an exhaustive, exposing, humiliating process,” he added.
   Judgments in liability cases generally cost facilities in the $500,000-$600,000 range, Bates said.

   The following, he said, are the top 10 reasons for lawsuits involving premises security, and how hospitals can avoid them:

   1. Failure to assess and respond to risks
      Be sure your security program meets the needs of your security will put your security program under a microscope, Bates said. “It’s an exhaustive, exposing, humiliating process,” he added.
      Judgments in liability cases generally cost facilities in the $500,000-$600,000 range, Bates said.

   The following, he said, are the top 10 reasons for lawsuits involving premises security, and how hospitals can avoid them:

   1. Failure to assess and respond to risks
      Be sure your security program meets the needs of your

The most basic activities that hospital security directors and their officers perform help protect hospitals against lawsuits, said Norman D. Bates, Esq., president and founder of Liability Consultants, Inc., in Boston.

By assessing security risks and responding, hospital security programs help maintain safe facilities and protect patients, visitors, and staff members. And by knowing the reasons commonly behind lawsuits, security directors can learn from the experiences and mistakes of others who have been sued for inadequate security measures, and develop more effective programs themselves, said Bates, who spoke during the International Association for Healthcare Security and Safety annual meeting in Boston in June.

Although hospitals cannot prevent all crime, the basic rule is that property owners are required to maintain reasonably safe premises in light of the risk of crime, Bates said.

Going to court and having to defend your hospital’s security program is an unenviable task. A court case that alleges inadequate security will put your security program under a microscope, Bates said. “It’s an exhaustive, exposing, humiliating process,” he added.

Judgments in liability cases generally cost facilities in the $500,000-$600,000 range, Bates said.

The following, he said, are the top 10 reasons for lawsuits involving premises security, and how hospitals can avoid them:

1. Failure to assess and respond to risks
   Be sure your security program meets the needs of your

Editor’s note: Each issue of Healthcare Security Alert features an expert’s answers to your security questions. Steven MacArthur, safety consultant for The Greeley Company, a division of HCPro, Inc., in Marblehead, MA, answers this month’s question. If you have a security question for one of our experts, e-mail Senior Managing Editor Joanne Finnegan at jfinnegan@hcpro.com.

Q Our hospital is considering using an overhead paging code that would warn our staff when a suspicious person has been observed in the building. We would use this code to cover not only suspicious individuals who fit the profile for child abductors, but other circumstances as well. What are other hospitals doing along these lines? Do they have an overhead paging alert? If so, how does it work and what is the staff’s expected response?

A I have not encountered hospitals that use a suspicious-persons code, and to be honest, I’m curious about how a facility would operationalize such a process.
facility, said Bates. You need to assess risks and respond to them. For instance, an apartment complex in Atlanta was sued for $9 million after a woman was raped there. Her attorney detailed a previous rape that had occurred at the complex and showed that the owners had done nothing to prevent another crime from happening, he said.

The simple lesson is that when you have an incident occur, look at what you can do to prevent a future problem. Be sure to gather crime data at your facility and analyze the information. Keep track of complaints and consider security risks inherent to the healthcare industry. Conduct these assessments on a regular basis.

A reduction in security resources
Sometimes budget cuts are necessary. Your hospital may be looking at facilitywide cuts to create cost savings. But before a hospital considers a cut to its security program, ask the following: Can you do it in a way that is logical and defensible? said Bates. Consider the losses prevented and reduction in incidents by having a good security program in place.

Be sure to evaluate trends in crime before making any cuts. For instance, before you cut a security guard on the night shift, look at your data, which may show that the highest risk for crime occurs at night. Weigh alternatives when deciding how to implement cuts. If you need to reduce the staff, perhaps you can add security cameras. If you must have fewer security officers on patrol, maybe maintenance workers can check for security risks, such as lights that are burned out.

Insufficient staffing
Be sure to look carefully at staffing levels at your facility to ensure that they are adequate and that you put people where they are most needed, Bates said. The following factors can get facilities in legal trouble:

- Poor allocation of resources
- Inadequate number of staff members
- Too many nonsecurity tasks that detract from officers’ primary function
- Failure to analyze job tasks and where time is spent

Negligent hiring
Ensure that your facility adequately screens potential employees before hiring them, Bates said. If an employee commits a crime, a facility will have a problem if a proper background check was not done. For example, a nursing home could find itself in court if a nursing assistant commits a rape and the facility failed to conduct an adequate background check that would have revealed a history of violence.

Be sure to do the following:

- Assess the risk of the position that an employee will hold
- Make sure that the extent of your background investigation is in proportion to the risks involved
- Check a potential employee’s criminal history, because failure to do so is a major cause for liability
- Document your investigation

Negligent retention
As well as being careful during the hiring process, hospitals should not ignore an employee who has demonstrated problem behavior, Bates said. As an example, he cited the liability that a company faced when an employee killed six coworkers.

Hospitals should think twice before they continue to retain an employee who:

- Has a history of violence or excessive force
- Continues to violate company policies, rules, and procedures
- Has been convicted of a crime during job tenure that would have precluded the employee from being hired initially
- Shows poor judgment in handling security incidents

Negligent supervision
“These are so basic,” Bates said, about ensuring adequate supervision of your security staff. You can face liability if an employee deviates from his or her responsibilities because supervisors weren’t ensuring that the person was doing the job. For instance, if a security guard is not doing his rounds, and an incident occurs, a plaintiff’s attorney could use that against a hospital.
Bates cited the case of a hotel guard who took a break from his rounds while a hotel patron was raped in a fire lane near the front entrance of the facility.

The following mistakes can create a liability:

- Failure to provide adequate amounts and/or types of supervisions to ensure that staff members are conducting security patrols and tasks as required
- Failure to address a staff member’s prior performance or behavior through your disciplinary process
- Failure to maintain accountability, such as poor key control

**Insufficient training**

Be sure you provide security staff members with adequate training to ensure that they are familiar with all aspects of their job.

Consider the actual job that security personnel perform, Bates said. If you have analyzed the job, consider how much time a security officer is actually spending on various tasks.

Be sure that your training corresponds to the workload. For instance, if 25% of service calls at a hotel were for medical assistance, it is appropriate to look at how much training personnel receive in first aid and responding to medical emergencies, said Bates.

The following can create problems:

- Failure to provide competent and experienced trainers
- Failure to retrain an employee after the poor performance of a task
- Failure to train staff members in the skills needed as new responsibilities are added
- Failure to provide training levels and amounts proportionate with job responsibilities

**Violation of industry standards**

You need to be aware of industry standards for your security program, Bates said. Failure to comply with those standards can provide strong evidence of negligence on the part of your hospital, he said. On the other hand, if you follow those standards, it can be a great defense in a court case.

Hospital security directors should be aware that the National Fire Protection Association (NFPA) has established security guidelines for healthcare facilities, he said.

The NFPA publishes a *Guide for Premises Security*, also known as NFPA 730 (see the March issue of *Healthcare Security Alert* for more information), and NFPA 731, a standard for the installation of electronic premises security systems.

**Violation of your own standards**

If you are not following your own standards, this can be even further evidence of negligence, Bates said.

However, be careful what standards you set, and be sure you can meet them. Standards can be problematic when they are too inflexible.

For instance, your operations manual may state that a security officer shall monitor the parking lot continuously. But what happens if that officer is called away to respond to a gang fight in your ER? “Take a close, hard look at your policies,” Bates said. “Is it something you can live up to?”

Joint Commission surveyors frequently use this approach when checking on a hospital’s policies.

**Security equipment or technology failures**

Security equipment can reduce your risk of liability, but you need to be sure that it works properly. Was a lock broken that allowed an attacker into your facility? Did poor key control allow access to someone not welcome at your hospital? Were cameras not working when an assault occurred?

The following can create liability:

- Broken/inoperative equipment
- Out-of-date technology
- Systems that no longer meet industry standards
- Equipment that fails to comply with laws, codes, or standards
- Missing equipment
- An insufficient amount of equipment, such as too few cameras or no tape deck to record activities
In my experience, hospitals employ emergency codes to enlist a response to a specific type of occurrence, such as a fire, infant abduction, utilities disruption, internal disaster, or external disaster. First, you would need to define what constitutes a suspicious person and then define at what point that person would become worthy of proactive management.

Think about the following concerns:

- When do you call a code? For example, there might be any number of visitors in your facility who might fit the profile of a child abductor. Do you call a code if a suspicious person goes to your maternity unit or walks by the unit, because they might be casing the unit?
- Who do you empower to pull the trigger and activate a code? At what point do you want folks to actually set the alert into motion?

One concern of mine is that you might create a precipitous response.

I can’t help but think that the process you describe wouldn’t provide enough information, such as the location of the person or a description, to inform an appropriate response. This might prompt a more panicked reaction than you’d want to invoke. And to engineer out the likelihood of overresponse would require a great deal of education, such as how to profile suspicious people and what is an appropriate response.

I would recommend your hospital fold this type of occurrence into whatever alert system you have in place for a security condition.

If the purpose of this code is to attain some sort of heightened vigilance, I’m not quite sure how you would be able to scale a response to that level. From my experiences managing security, I think the best way to manage these types of situations is to identify a means in which the individual who identifies a suspicious person can quickly contact security and allow your security force to respond.

I would advise you to work with what you have for security alerts and try to build something from that angle, rather than come up with an additional process.

As long as folks have a means of summoning assistance when they’re in trouble, you should be able to manage interlopers in your facility.