



# BRIEFINGS ON HOSPITAL SAFETY

Your trusted source for hospital safety compliance

## Staff training needed for OSHA compliance

### Can save you violations, fines

William Morgan, SASHE, CHFM, knows the importance of training.

He is reminded of it every day because of the location of his state's OSHA office: directly across from St. Alphonsus Regional Medical Center in Boise, ID, where he is the engineering manager.

The OSHA inspectors frequently eat lunch in the hospital's cafeteria, and they keep their eyes open during their visits, Morgan says. During one visit, they spotted two hospital workers repairing the light on an ambulance sign while standing on the roof without any safety restraints, rather than putting up a ladder to reach the sign.

"They cited us for it," says Morgan. However, the hospital had just completed a training session in ladder safety less than a week before. Morgan was able to show that the two workers had just attended training and were not following the hospital's policy and procedures.

As a result, St. Alphonsus was able to get the citation removed along with the fine that went with it, Morgan says. It's just one example of how training can pay off, he notes.

### Some obstacles to training

OSHA standards require hospitals to train their employees as part of the global "occupational safety and health" needs of the workplace, but managing that training is sometimes a challenge, Morgan says.

For one, training takes time. In the current tough economy, hospitals have downsized and added more duties to hospital safety officers, many of whom find themselves

**"There are a lot of 'gotchas' in OSHA with documentation."**

—William Morgan,  
SASHE, CHFM

managing new departments, he says. Managers who are doing more and more work have little time to plan and implement training sessions.

The time hospitals can allot for education has decreased, particularly for the orientation process, agrees **Steve MacArthur**, safety consultant for The Greeley Company in Marblehead, MA. "Where in the past safety officers might have had a couple of hours [for training], now they have but an hour or less," MacArthur says.

For some safety officers, there is also a lack of knowledge about training, Morgan says. Particularly in smaller facilities, talented workers are promoted to managerial positions. "They don't have a real strong background in management or administration," he says.

However, hospitals face serious problems if they are targeted for an OSHA inspection and do not have training programs in place. "You have a responsibility to protect your staff from a safety perspective, and it is good business practice," Morgan says.

#### IN THIS ISSUE

**p. 4 Sample safety training policy**  
Use this sample policy to outline how your facility will provide safety training.

**p. 5 Eight steps to plan emergency exercises**  
Learn about eight ways to improve your emergency planning.

**p. 8 Keep an eye on digital cameras**  
We detail the lessons learned from an Arkansas hospital's recent privacy breach due to a stolen digital camera.

**p. 10 2010 BHS story index**  
Use our handy index to find any article from last year.

**p. 12 A new twist on fire extinguisher training**  
A South Carolina hospital uses technology to train staff on how to use fire extinguishers.

HCP Pro

## Staff training

< continued from p. 1

### Develop a training program

At St. Alphonsus, there are two kinds of training—what Morgan calls compliance training and craft training.

Compliance training focuses on safety, the need to train new employees, new equipment, hazardous materials, and changes to processes. Craft training focuses on the tricks of the trade when it comes to carpentry, electrical, plumbing, and HVAC, says Morgan. This training focuses on day-to-day repairs, new products, new policies, hospital system

changes, and discussions about those systems. “You could have thousands of topics,” he says.

Compliance training is essential for new employees, Morgan says. “When you are bringing new employees in, before you turn them loose to do a job, they need to know the risks of the job. They need to be trained how to do it.”

OSHA has published booklet 2254 to help hospitals develop the training programs needed to manage worker safety. The guidelines provide support information but are not a code that you must follow, Morgan notes.

The OSHA training guide model follows these steps:

- Determine whether training is needed
- Identify training needs
- Identify goals and objectives
- Develop learning activities
- Conduct the training
- Evaluate the program’s effectiveness
- Improve the program

### Training topics are numerous

There are several basic topics that correlate with the *Code of Federal Regulations (CFR)*, which is an enforceable code by OSHA, Morgan says. (See the sidebar on p. 3 for a list of those topics.)

Hospitals have to focus on the important regulatory issues—bloodborne pathogens, hazard communications, fire response, and workplace violence, MacArthur says. Then there are other topics to cover, such as lockout/tagout and respiratory protection. “It’s a most difficult thing to do completely,” he admits.

Your risk analysis will determine training topics for your facility, Morgan says. For instance, if you have a new facility and no asbestos in your buildings, you can cross that off your list.

In addition, consider the need to train staff on confined space walkthroughs, Morgan says. First, you need to identify the training requirement in a policy; you then must require training for all staff with duties under the

#### Editorial Advisory Board

#### Briefings on Hospital Safety

HCPPro

Group Publisher: **Emily Sheahan,**  
*esheahan@hcpro.com*

Senior Managing Editor: **Jay Kumar,**  
*jkumar@hcpro.com*

Editor: **Joanne Finnegan**

Contributing Editor: **Steven MacArthur,**  
Safety Consultant, The Greeley  
Company, Marblehead, MA,  
*smacarthur@hcpro.com*

**Barbara Bisset, PhD, MS, MPH, RN**  
*Executive Director*  
Emergency Services Institute/WakeMed  
Raleigh, NC

**Joseph Cocciardi, PhD, MS, CSP, CIH**  
*Cocciardi & Associates*  
Mechanicsburg, PA

**Leo J. DeBobes, MA (OS&H), CSP, CHCM, CPEA, CHEP, CSC, EMT**  
*Assistant Administrator, Emergency Management/Regulatory Compliance*  
Stony Brook University Medical Center  
Stony Brook, NY

**Elizabeth Di Giacomo-Geffers, RN, MPH, CSHA**  
*Healthcare Consultant*  
Di Giacomo-Geffers and Associates  
Trabuco Canyon, CA

**Zach Goldfarb, EMT-P, CHSP, CEM**  
*President*  
Incident Management Solutions, Inc.  
East Meadow, NY

**Ray W. Moughalian, BS, CHFRM**  
*Principal*  
Saf-T-Man  
Methuen, MA

**John L. Murray Jr., CHMM, CSP, CIH**  
*Safety Director*  
Baystate Health  
Springfield, MA

**Paul Penn, MS, CHEM, CHSP**  
*EnMagine/HAZMAT for Healthcare*  
Diamond Springs, CA

**Dalton Sawyer, MS, CHEP**  
*Director, Emergency Preparedness and Continuity Planning*  
UNC Health Care  
Chapel Hill, NC

**Steve Schultz**  
*Corp. E&O Safety Director*  
Cape Fear Valley Health System  
Fayetteville, NC

**Barry D. Watkins, MBA, MHA, CHSP**  
*Senior EC Specialist*  
Corporate Safety  
Carolinas HealthCare System  
Charlotte, NC

**Kenneth S. Weinberg, PhD**  
*President*  
Safdoc Systems, LLC  
Stoughton, MA

**Earl Williams, HSP**  
*Safety Specialist*  
BroMenn Healthcare  
Bloomington, IL

**Pier-George Zanoni, PE, CSP, CIH**  
*ZLH Consulting*  
St. Johns, MI

Briefings on Hospital Safety (ISSN: 1076-5972 [print]; 1535-6817 [online]) is published monthly by HCPPro, Inc., 200 Hoods Lane, Marblehead, MA 01945. Subscription rate: Regular \$299/year or \$538/two years, Platinum \$499/year; back issues are available at \$25 each. • Briefings on Hospital Safety, P.O. Box 1168, Marblehead, MA 01945. • Copyright © 2011 HCPPro, Inc. All rights reserved. Printed in the USA. Except where specifically encouraged, no part of this publication may be reproduced, in any form or by any means, outside the subscriber's facility, without prior written consent of HCPPro, Inc., or the Copyright Clearance Center at 978/750-8400. Please notify us immediately if you have received an unauthorized copy. • For editorial comments or questions, call 781/639-1872 or fax 781/639-2982. For renewal or subscription information, call customer service at 800/650-6787, fax 800/639-8511, or e-mail: [customerservice@hcpro.com](mailto:customerservice@hcpro.com). Visit our website at [www.hcpro.com](http://www.hcpro.com). • Occasionally, we make our subscriber list available to selected companies/vendors. If you do not wish to be included on this mailing list, please write to the marketing department at the address above. • Opinions expressed are not necessarily those of BHS. Mention of products and services does not constitute endorsement. Advice given is general, and readers should consult professional counsel for specific legal, ethical, or clinical questions.

policy. This must occur before staff are assigned duties and any time you make a change to your policy. You want to train staff at least annually, he says.

Remember to train people if they change jobs or if you bring in a new piece of equipment. You also need to retrain staff if you observe that people are not following your policies and procedures, and then document that training.

"There are a lot of 'gotchas' in OSHA with documentation," Morgan warns. It is a good idea to have a sign-in sheet at training sessions to record staff participation.

Training documentation should include each employee's name, the signature of the trainer, and the date of training. Certification must be available for review by OSHA inspectors.

### Types of training

At St. Alphonsus, the medical center has monthly compliance training for its staff. New employees undergo a 90-day program in which they must complete all of the sessions. Some of that training involves reading policies and procedures online, whereas other training takes place in one-on-one sessions.

MacArthur says hospitals should not underestimate the value of that face-to-face training. Department-specific orientation and ongoing education can vary depending on the department, he says.

"Some tend to have a very robust process from beginning to end, while others, maybe not so much," he says.

Departments such as environmental and food services tend to have better results because everyone has a chance to hear the message and ask questions, MacArthur says. Staff also tend to be more invested in training when it comes to safety.

There are many ways to present your educational program, Morgan says. You can do training at group meetings, show films or videos, use PowerPoint® presentations, or conduct individual training.

You want to keep training clear and have measurable objectives. Review your policy, the individual responsibilities, your logs, safety equipment, and the location of sites.

Morgan offers a word of caution when it comes to online training. It would be wise to call your local or regional OSHA people to ask whether online training is acceptable, he says, since he has heard from OSHA offices that have questioned it. Get that approval in writing if possible as OSHA personnel can change.

### Other training tips

How can you determine your training needs? Consider what is needed to ensure safety, Morgan says. Look at what is identified in your policies and mandated by regulations. Train staff if injury or accident records show a need.

Morgan advises safety officers to take advantage of training resources. Use the Web and the free information

> *continued on p. 4*

### Basic safety training topics

There are a number of training topics that correlate with the *Code of Federal Regulations (CFR)*. The following is a list of those topics and the *CFR* reference:

- Asbestos: 29 CFR 1910.1001
- Bloodborne pathogens: 29 CFR 1910.1030
- Compressed gas: 29 CFR 1910.101
- Confined space entry: 29 CFR 1910.146
- Control of hazardous energy (lockout/tagout): 29 CFR 1910.147
- Employee emergency plans and fire prevention: 29 CFR 1910.038
- Fire extinguishers: 29 CFR 1910.157
- Hand and portable power tools: 29 CFR 1910.242
- Hazard communications: 29 CFR 1910.1200
- Hazardous waste emergency response: 29 CFR 1910.120
- Laboratory safety: 29 CFR 1910.1450
- Laundry machines and operations: 29 CFR 1910.264
- Motor vehicles: 29 CFR 1910.601
- Noise exposure: 29 CFR 1910.95
- Personal protective equipment: 29 CFR 1910.132
- Portable ladders (wood and metal): 29 CFR 1910.025 and 1910.026
- Respiratory protection: 29 CFR 1910.134
- Welding, cutting, brazing: 29 CFR 1910.252

## Staff training

< continued from p. 3

there. Additionally, there are many good companies that sell training packages you can purchase, he notes.

"I like to bring in vendors," Morgan says. For instance, a company that supplies personal protective equipment will come in for free and give a demonstration, he says. Use those experts to train your staff. Hospitals should also have a safety training policy, he adds. (See the sample policy below.)

There are many issues to worry about, but hospitals should not ignore training, he says. "Hospitals are running a lot of work. Staffing is tight. People are managing

so many things. Ultimately, the thing that gets pushed off the plate is training."

But if you haven't completed training and you have an accident on your site, a staff member is injured on the job, or someone reports a possible violation, you will face liability, Morgan says. Be sure you conduct an annual review of your training policy and plan, he says. If OSHA comes in to investigate, "the first thing they are going to do is ask about training. That's not why you do it. You do it to protect your staff, your visitors, and your patients. But that's the stick." ■

### Sample safety training policy

**Category:** Work procedures

#### Training

The engineering department will establish and maintain a training program to orient new employees and refresh existing employees to standard operating procedures. Training shall be incorporated into monthly department meetings where possible. All training will be documented in a master education listing as well as in the employee performance plan.

#### Procedure

- a. Training programs will be accompanied by an outline of the items discussed and a sign-in sheet.
- b. The supervisor of the participating trade will conduct the training sessions. This person may use any resources available (e.g., educational services, films, outside resources). Most resources are ongoing training items; cost should be kept to a minimum.
- c. Training is considered mandatory, and employees from other shifts will be compensated. Training sessions will be conducted at times that will minimize cost.
- d. Employees are expected to use the techniques and procedures presented and are invited to offer constructive suggestions on how to make training sessions more valuable.
- e. Mandatory training sessions include, but are not limited to, the following topics:
  - Fire response team protocols
  - Asbestos awareness
  - Hazard communications
  - Hazardous waste
  - New employee orientation
  - Infection control
  - Disaster training

Source: William Morgan, SASHE, CHFM, engineering manager, St. Alphonsus Regional Medical Center, Boise, ID.

## Follow these eight steps to design your emergency exercises

### A recipe for success

Hidden within the hundreds of pages of government documents on emergency planning, there's a recipe for designing emergency exercises, says **Marge McFarlane, PhD, MS(ENPH), CHSP, HEM, MEP.**

"I'm a laboratory person; I love a recipe," says McFarlane, who began her career in healthcare as a laboratory safety officer and is now an independent safety consultant who runs Superior Performance, LLC, in Eau Claire, WI.

It was in her role with the Wisconsin Hospital Emergency Preparedness Program as the Department of Homeland Security Exercise and Evaluation Program (HSEEP) coordinator that McFarlane took on the job of "translating" those government documents.

Within the hundreds of pages of HSEEP documents is an eight-step model hospitals can use to design, conduct, and evaluate their emergency management exercises, which are required by The Joint Commission, Centers for Medicare & Medicaid Services, and to be eligible for federal grant money, McFarlane says.

It's help most hospitals can use, she notes. A 2008 survey of Wisconsin hospitals identified a number of barriers to designing emergency exercises. Hospitals said they face a lack of planning time, training in exercise design, tools and templates, and personnel to assist in the planning process. (See p. 7 for an excerpt from an exercise design checklist. The full checklist is posted in the **Hospital Safety Center** Forms Library at [www.hospitalsafetycenter.com](http://www.hospitalsafetycenter.com).)

### Eight is enough

According to McFarlane, following these eight steps can make the planning process easier:

**1. Base your emergency exercises on your needs assessment.** Look at your hazard vulnerability assessments and previous exercises to determine what you need to test or retest, McFarlane says. A hospital's after-action reports, in which emergency exercises are assessed, always identify areas for improvement.

Take a look at any disasters or emergencies that occurred at your facility and consider what went well and what didn't, she says. This could be a flood, a tornado, a hurricane, or an ice storm. Also, look at any new equipment your facility bought and think about incorporating it into a drill to test the training you've provided to staff, she says.

One purpose of conducting exercises is to validate your plans, policies, and procedures, as well as your training, McFarlane says.

**2. Determine the scope of your exercise.** Answer the questions of who, what, where, when, and how, says McFarlane.

**3. Write your statement of purpose.** This summarizes your needs assessment and the scope of your planned exercise. This will provide a framework for scenario development and what events will occur in your exercise, McFarlane says.

Your statement of purpose should state *who* should do *what* under *what conditions* and according to *what standards*, she says.

The Joint Commission identifies six critical areas for emergency management in its standards: communications, resources, safety and security, staff roles and responsibilities, utilities, and patient care/staff support. The government calls the areas "target capabilities," but it and The Joint Commission are both talking about the same issues, says McFarlane.

**4. Create SMART objectives.** "When you write objectives, make them SMART," says McFarlane. What does this mean? You want to write objectives according to this acronym. They should be:

- **Simple:** straightforward and easy to read
- **Measurable:** specific and observable
- **Achievable:** within the duration of the exercise
- **Realistic:** reflect actual goals of time, personnel, and resources
- **Task-oriented:** specific operations that are timely

> *continued on p. 6*

## Emergency exercises

< continued from p. 5

Here's an example of how to write SMART objectives: You decide your emergency exercise will be a mass casualty with the need for decontamination of victims. You want to focus on two critical areas or capabilities: communications and staff roles. When it comes to measuring how capable your organization is regarding communication during an emergency, outline what sub-capabilities you want to test, McFarlane says. For instance, your exercise can test how well communications go when it comes to notifying your ED of the incident, the notification to activate your incident command, your situation briefings, patient information management, and media inquiries.

Your objective is to look at how effective communications were during the exercise. Ask questions such as: To whom did staff communicate? Were there internal communications? Were there external communications? How do you evaluate success?

You want to write a SMART objective such as the following: Was the ED notified within 15 minutes of the external incident by the 911 emergency center? The answer is either yes or no.

To measure the effectiveness of the notification to activate your incident command, ask specific questions. Did the ED report to the hospital supervisor include a description of the incident? Determine the need for specialized resources? Note the initial actions being taken? Give the number of injured expected? Provide an estimated time of arrival and describe the criticality of the victims? Outline the nature and quantity of additional resources required?

Your second goal is to measure the capability of staff roles. Again, outline the sub-capabilities you want to test, such as the setup of your incident command, the ability to secure facility access, and how well you prepared for patient decontamination.

**5. Write a narrative.** Always write the objectives first and then the story, McFarlane says. You want to create a scenario that tests the objectives you choose.

Pick a scenario that could really happen, she advises. In Wisconsin, for instance, a snow or ice storm is a likely event, but a tsunami is not realistic.

Your scenario should be risk-based, realistic, and challenging, says McFarlane. It should contain three basic elements: conditions, context, and technical details. For example, your scenario may be that your community has had heavy rains and the nearby river is rising. It may reach flood stage in 48 hours. Your exercise may focus on an evacuation. Where will patients go if they need to be moved out of the facility? How will you get them to another location?

**6. Identify major and detailed events.** You want your emergency exercise to challenge staff. Have a list of activities you expect to happen. Plan for messages that move the action and provide information to drive objectives, McFarlane says. You want to create an escalating scenario that tests staff knowledge and skills as well as resources, she adds. For instance, you are planning a hospital evacuation when the facility suddenly loses power. As a result, your staff can no longer use the elevators to move patients. How can they carry patients down stairways? What about patients on ventilators? What happens if water is lost? How do you communicate if phone lines go out?

**7. Identify expected player action(s) based on your objectives.** What do you expect to observe during the course of the exercise? What do you hope staff will do when you give them the scenario and the timeline of events?

Keep in mind that all of the objectives do not need to be met within the first 30 minutes of the exercise, McFarlane says.

**8. Write messages based on the responses of participants.** This can keep the scenario on track, says McFarlane.

You may need to write corrective messages during the course of the exercise to move the scenarios along and to bring staff members back on task. ■

## Exercise design checklist excerpt

Adapted from: *Tool for Evaluating Core Elements of Hospital Disaster Drills*  
 AHRQ Publication No. 08-0019, June 2008

**Working exercise title:** \_\_\_\_\_

### Exercise planning team members

Name	Phone	E-mail	Organization

### I. Scope of exercise: Who will participate, what, where, when?

a. Select the type of exercise your hospital is performing. (Check one.)

1.  Tabletop exercise (discussion-based exercise, appropriate for 96-hour discussion)  
 Functional exercise (operations-based exercise with some simulated activities)  
 Full-scale exercise (operations-based exercise in real time)  
 Other (specify): \_\_\_\_\_
2.  Single facility  Communitywide  
 Regional  Other \_\_\_\_\_

b. Determine what the exercise scenario will include. (Check all that apply.)

(This is based on the Hazard Vulnerability Assessment. Hospital Incident Command System [HICS] reference documents can be found at [www.emsa.ca.gov/HICS](http://www.emsa.ca.gov/HICS); select appendix H.)

- |  |  |
|--|--|
| <input type="checkbox"/> Biological agent                                  | <input type="checkbox"/> Chemical agent              |
| <input type="checkbox"/> Fire  | <input type="checkbox"/> Incendiary device/explosive |
| <input type="checkbox"/> Natural disaster (e.g., tornado)                  | <input type="checkbox"/> Radiological agent          |
| <input type="checkbox"/> Structural collapse                               | <input type="checkbox"/> Transportation accident     |
| <input type="checkbox"/> Internal hospital system failure (specify): _____ |  |
| <input type="checkbox"/> Other (specify): _____                            |  |

c. Identify the main objectives (also known as target capabilities or critical areas) to be evaluated during the exercise.

(Check all that apply.)

- |   |  |  |  |
|---|--|--|--|
| <input type="checkbox"/> Decontamination                    | <input type="checkbox"/> Treatment         | <input type="checkbox"/> Biological illness exposure       | <input type="checkbox"/> Incident command    |
| <input type="checkbox"/> Triage                             | <input type="checkbox"/> Chemical exposure | <input type="checkbox"/> Equipment and supplies            |  |
| <input type="checkbox"/> Patient documentation and tracking |  | <input type="checkbox"/> Personal protective equipment use |  |
| <input type="checkbox"/> Rotation of staff                  | <input type="checkbox"/> Staffing          | <input type="checkbox"/> Zone operations                   | <input type="checkbox"/> Sheltering in place |
| <input type="checkbox"/> Communication and information flow |  | <input type="checkbox"/> Facility engineering              | <input type="checkbox"/> Patient flow        |
| <input type="checkbox"/> Radiation exposure                 | <input type="checkbox"/> Security          | <input type="checkbox"/> Surge capacity                    | <input type="checkbox"/> Evacuation          |
| <input type="checkbox"/> Other _____                        |  | <input type="checkbox"/> Other _____                       |  |

Source: Marge McFarlane, PhD, MS(ENPH), CHSP, HEM, MEP, Superior Performance, LLC, Eau Claire, WI. Used with permission.

## Stolen camera creates privacy breach for Arkansas hospital

Hospitals worry about laptop computers and other portable devices that contain patients' protected health information (PHI) being stolen. But what about digital cameras?

Such a device caused a privacy breach in October 2010 at an Arkansas hospital.

A stolen digital camera that contained photographs and newborn babies' personal information resulted in the breach at The University of Arkansas for Medical Sciences (UAMS) in Little Rock. Someone stole the camera from the pocket of a nurse's lab coat October 12, according to a posting on the UAMS website.

"It's not surprising," says **Chris Apgar, CISSP**, president of Apgar & Associates, LLC, in Portland, OR, because many people would not think of a digital camera as a security risk.

"Many healthcare organizations do not take into account all of the places PHI is stored, such as on a digital camera, copy machines, fax machines, biomedical equipment, and so forth, and [do not] recognize it as a security risk," says Apgar, a consultant who advises healthcare organizations about Health Insurance Portability and Accountability Act of 1996 (HIPAA) security compliance.

What do healthcare organizations need to worry about? "Just about anything electronic that can store data," Apgar says.

At UAMS, nurses took photos of the newborns for security purposes in case of abduction, the hospital said in a FAQ posting on its website ([www.uamshealth.com/breach](http://www.uamshealth.com/breach)). The hospital did not respond to a request for further comment on the incident.

### What happened

Hospital staff took the pictures so that in the unlikely event of a kidnapping, a photograph would be available for law enforcement. The National Center for Missing & Exploited Children ([www.missingkids.com](http://www.missingkids.com)) recommends such a practice, the hospital said.

A nurse carrying the camera was called into surgery and, although her lab coat was in a restricted area,

someone gained access to it and stole the camera, the hospital said.

"Generally, a theft like this occurs because the person taking the camera simply wants the camera, not the information contained on it," the university said in the FAQ.

**Fredrick G. Roll, MA, CHPA-F, CPP**, president and principal consultant of Healthcare Security Consultants, Inc., and Roll Enterprises, Inc., in Frederick, CO, agrees the thief probably wasn't interested in the information. But once someone has taken that information, the hospital can't be sure what will happen to the data, Roll notes.

Staff took photos of the newborn babies between July and October 2010. The accompanying patient labels included the baby's and mother's names, birthdays, address, telephone number, insurance status, medical record numbers, and physician names, according to a report by the Associated Press. The hospital said the pictures did not contain Social Security numbers. But because the information is part of the patient record, it falls under HIPAA, Roll says.

### A privacy and security breach

The university told parents on its website that because the camera contains demographic information, there is a chance someone might misuse the information, although it was not aware of anyone doing so.

The hospital recommended that any patients worried about identify theft contact the three credit reporting agencies to obtain a copy of their credit report and place a fraud alert on file.

"We are sorry this incident occurred. Unfortunately, theft does occur despite our attempts to prevent it," the hospital told patients in its FAQ.

The hospital said police are still investigating the case and trying to recover the camera. Police have conducted interviews and reviewed security camera footage.

In addition to notifying law enforcement, UAMS said on its website that it self-reported the incident to the Office

for Civil Rights, the federal agency that investigates HIPAA incidents, which it said will also conduct an investigation.

### A lesson for staff

UAMS said it is reminding staff about the need to secure items such as cameras. It also plans to remind staff about the need to delete images from cameras after downloading them to a secure computer.

If hospitals are using digital cameras to take patient photos and information, “obviously you need to take care of it,” says Roll.

As soon as a photo is taken, staff should store it onto a hospital’s electronic health record or some other managed system and remove it from the camera, says **Christopher Hourihan**, manager of common security framework development and operations at HITRUST, the Health Information Trust Alliance in Frisco, TX.

Apgar agrees to a point. “It is not always feasible, especially in a busy maternity ward, to immediately load the picture to the electronic medical record and destroy the image from the usual storage card in the camera. True ‘deletion’ requires formatting the flash card. Deleting the picture from the camera or flash card does not destroy the image, and it can be recovered,” he notes.

The hospital said it is reviewing all of its policies and procedures involving photographs of patients to ensure that it makes every effort to prevent such an incident from occurring again.

UAMS followed many of the typical steps taken after a privacy breach, sending letters to notify families whose babies’ pictures may have been on the camera.

The hospital set up the FAQ page to provide answers to patients and the public. Parents with further questions or concerns can also call the hospital’s HIPAA hotline. The hospital says it did not include any clinical information with the photos. Part of the problem, however, is that the facility does not know which photos were on the camera or how many families were affected.

The camera contained photographs of some, but not all, babies born at the hospital from July through October, UAMS said. Hospital staff deleted some pictures from the

camera, but the facility doesn’t know which ones. “There is no way we can be 100% sure if your baby’s picture was on the camera,” the hospital said on its website.

### A warning to others

The Arkansas case can be a wake-up call to other healthcare organizations.

“It does highlight a factor we often see lacking in risk assessments,” says **Frank Ruelas**, director of compliance and risk management at Maryvale Hospital in Phoenix and principal of HIPAA College in Casa Grande, AZ. In many risk assessments, healthcare organizations do not look beyond the obvious risk factors to consider items such as digital cameras, Ruelas says.

The use of digital cameras isn’t limited to nurses in the infant nursery, he says. An infection control nurse may use one to document practices she sees on your hospital floors. A wound care nurse may use a camera to document the stage of a pressure ulcer. Different departments may have their own cameras, or they may borrow another department’s camera when they need it.

“It’s really a Pandora’s box,” Ruelas says, with no one sure just what information a particular camera contains.

Organizations should require staff members to pull the flash card—which stores the images—after they use it, format the flash card, and put it back into the camera with the data removed, Apgar says. Staff need to put a blank flash card in the camera so data are not on the device itself, he adds.

However, even with the best policies and procedures in place, staff might not always follow them, says Ruelas. Ideally, staff members should delete the photographs at the end of their shift after downloading them. But are you confident that will always happen?

To prevent human error, Ruelas advises organizations not to allow a lot of storage on devices such as digital cameras or USB drives. It is only a matter of time before a device is lost, he says. A camera without the flash card that allows for storage may only hold 10 pictures. When the camera is full, staff must delete photographs or download them onto a server or intranet. ■

## Briefings on Hospital Safety 2010 index

### Emergency management

The benefits of customizing your HICS position chart.

April, p. 6.

The big eight issues to disaster recovery. Sept., p. 8.

Boston hospital conducts NICU evacuation drill. Nov., p. 10.

Children pose special challenges for emergency planners.

Oct., p. 6.

Flooding causes chaos in hospital distribution system.

Dec., p. 8.

Get your hospital back on its feet after a disaster. July, p. 9.

GIS mapping technology strengthens emergency prep.

Jan., p. 3.

HVA events will let surveyors test your flexibility. May, p. 7.

Include HIPAA privacy officers in your emergency planning.

Dec., p. 6.

New tool lets you download and customize paper patients.

Feb., p. 4.

Options for corpse storage during emergency response.

April, p. 1.

Prepare for the worst with repetition. Oct., p. 1.

Sample unit isolation plan for emergency response.

May, p. 10.

Tip of the month: Use these ideas to improve vertical

evacuations. Feb., p. 12.

### Environmental compliance

ASHE winner discusses the future of green construction.

Jan., p. 7.

### Fire protection

Get staff to help in the fight against corridor clutter. Dec., p. 4.

An inside look at a CMS *Life Safety Code*® survey. Sept., p. 1.

Involve hospital leaders in solving this top survey problem.

Dec., p. 12.

Three solutions to corridor clutter. Dec., p. 3.

### Infection control

California hospital hit with major fine for violating the ATD standard. July, p. 1.

Don't put your lab at risk; check on proper PPE use.

June, p. 10.

Include water fountains on your *Legionella* hit list. June, p. 12.

Investigate federal waivers to help your H1N1 response.

Feb., p. 9.

FDA approves new Steris System 1 alternative. June, p. 8.

FDA: Hospitals have 18 months to replace SS1. April, p. 10.

OSHA considers infectious disease standard. Dec., p. 10.

Seek Steris SS1 replacement and watch for any updates.

Feb., p. 1.

Study shows surgical teams still at risk for accidental sharps injuries. Aug., p. 6.

Tie EC and IC together to create a safe environment.

Sept., p. 5.

Union and hospital system cooperate on pandemic pact.

Jan., p. 9.

### The Joint Commission

Clarifying mis-scored life safety citations can give your survey a second chance. Aug., p. 9.

EC risk assessment important part of suicide prevention.

June, p. 9.

EC scoring may herald survey compliance pitfalls. April, p. 5.

How ILSMs can compensate for life safety deficiencies.

Nov., p. 5.

How to comply with three problematic standards. Aug., p. 1.

It's okay if facilities don't have perfect EC processes. June, p. 7.

Joint Commission backs off of emergency prep tracers.

June, p. 1.

Joint Commission notebook: Verify fire response plan roles under EC.02.03.01. March, p. 5.

Joint Commission removes certain MOS provisions. July, p. 11.

Joint Commission survey results for first half of 2010.

Nov., p. 1.

New kid on the top five list: LS.02.01.30. Nov., p. 4.

Resolve to improve your life safety programs in 2010.

Jan., p. 1.

Reviewing new ambulatory EC standards reveals MRI and diagnostic imaging best practices for hospitals. June, p. 3.

Survey monitor: EM is no longer just a couple of surveyor questions. July, p. 4.

Survey monitor: Joint Commission spends five days at Midwest health system. Dec., p. 1.

Survey monitor: Past tabletop efforts rewarded during emergency session. April, p. 8.

Survey monitor: Top-cited standard reveals rift with clinical activities. March, p. 8.

Surveyor questions focus on six critical areas of EM. July, p. 7.

Think beyond D icons for your EC documentation. May, p. 1.

Tip of the month: Involve leadership in solving your corridor clutter. Sept., p. 12.

### Medical equipment

Review FDA recommendations for CT scanners. March, p. 6.

Tip of the month: Consider using a hospital's new MRI safety steps. April, p. 12.

### Miscellaneous

Healthcare reform items for safety committees to review. June, p. 6.

How to address *Life Safety Code*<sup>®</sup> survey deficiencies. Oct., p. 7.

Identifying impairments to life safety systems. Nov., p. 9.

Time for facility safety officers to get on board with performance improvement. Oct., p. 11.

### OSHA compliance

Bloodborne retains top spot, lockout/tagout spikes. March, p. 1.

Ideas on how to discipline workers for OSHA violations. May, p. 8.

OSHA notebook: Be careful with distinctions about N95 shortages. Feb., p. 6.

OSHA Q&A tackles H1N1 shots, respirators, and more. April, p. 11.

State OSHA agency fines hospital for alleged H1N1 slips. May, p. 6.

Tip of the month: Use OSHA bulletin to reinforce accelerator safety. Jan., p. 12.

### Security

After the attack: MGH security shares experience. April insert.

Annual security assessments become California law. June insert.

Best practices for healthcare security. Jan. insert.

Exploring access control systems. Aug. insert.

Five precautions to help prevent violence in your ED. March insert.

How can non-safety staff members become involved in surveillance? April insert.

How to handle psych and forensic patients. Dec. insert.

Hurricane season brings security challenges. June insert.

Johns Hopkins shooting grabs national attention. Dec. insert.

Patient surge and security planning. Oct. insert.

Preparing for a high-profile forensic patient. March insert.

Preventing drills that go too far. Sept. insert.

Protecting ED staff members from violence. Nov. insert.

Questions of the month: How do I assess my hospital security camera system? May insert.

Questions of the month: When hiring security, what should I look for, both in certification and personality? Feb. insert.

Suspicious woman at MPMC later attempts kidnapping. July insert.

Telling the disgruntled from the dangerous. May insert.

Think past 'big city' risks to defend against terrorism. Feb. insert.

Threat assessment team helps protect employees. Jan. insert.

TJC releases Sentinel Event Alert on violence. Aug. insert.

Visitor badge program a hit at South Carolina hospital. July insert.

What are some security measures to consider during a natural disaster? Nov. insert.

What do my security officers need to know about handling unruly patients? Sept. insert.

What do we have to consider before deciding whether security should carry stun guns? Oct. insert.

When staff members become a security threat. March insert.

### Workplace health and safety

Actions you can take to stave off bedbug infestations. Jan., p. 6.

An early look at a new position: Sustainability manager. March, p. 10.

Managing laboratory safety in your hospital. Sept., p. 11.

Promote widespread discussion about blunt-tip sutures. Feb., p. 7.

Tip of the month: FDA warns of StatSpin centrifuge problems. May, p. 12.

Tip of the month: Keep tabs on proposed humidity range reductions. March, p. 12. ■

## Virtual fire extinguisher provides realistic training

Imagine you have just discovered a hot, smoky fire. You grab a nearby fire extinguisher, but then you hesitate. You've never actually used a fire extinguisher before.

It's a situation that staff members at Spartanburg (SC) Regional Medical Center won't have to worry about.

Thanks to a Spartanburg Regional Foundation grant of approximately \$12,000, the medical center is using new technology to teach healthcare workers how to put out a fire. The BulLEX system includes a laser-powered fire extinguisher and digital flames that simulate a real fire and are tough to put out.

**Douglas Neubauer**, the hospital's employee safety specialist, says he plans to eventually train the more than 5,000 employees in the Spartanburg health system. He has already trained some departments, and new hires are now receiving the training as part of their orientation. "I hope they never have to use it, but if they do, they can be confident," Neubauer says.

### Generating employee confidence

Using the virtual fire extinguisher, which has a realistic weight and feel, to douse the digital flames has removed employees' doubts. That was the experience of Mary Kinnunen, an administrative assistant at the hospital, who used the training device. "I have a fire extinguisher sitting in my pantry, and I always didn't know

what I'd do," she told television station WYFF4. But using the virtual fire extinguisher was easy, Kinnunen said. "It actually amazes me. I kind of want to laugh because I've always been scared of it. Now I know that I can do it," she told a television reporter.

Training is taking place department by department, Neubauer says. The technology helps hospitals bring a realistic approach to training staff using PASS:

- Pull the pin
- Aim the nozzle at the base of the flames
- Squeeze the trigger while holding the extinguisher upright
- Sweep the extinguisher from side to side and outward to extinguish flames

"When you're expecting your staff to respond to a fire, and we want to get it out before it gets too big, then you need to be able to apply the hands-on training for them, and this device will do it," he says.

Neubauer is a reserve deputy fire marshal for the city of Spartanburg. When the fire department offers fire safety training to the public, it encounters many people who have never used an extinguisher and are not sure how to operate one. "I thought, 'We have several thousand employees, and it could be one of our people' " who hesitate when faced with a real fire. ■

<b>Hospital Safety Center Subscriber Services Coupon</b>				
<input type="checkbox"/> Start my subscription to <a href="http://www.hospitalsafetycenter.com">www.hospitalsafetycenter.com</a> immediately.				
Options	No. of issues	Cost	Shipping	Total
<input type="checkbox"/> Regular	12 issues	\$299 (BHSPE)	\$24.00	
<input type="checkbox"/> Platinum	12 issues plus full Web access	\$499 (BHSE)	\$24.00	
<b>Order online at <a href="http://www.hcmarketplace.com">www.hcmarketplace.com</a>. Be sure to enter source code N0001 at checkout!</b>		<b>Sales tax</b> (see tax information below)*	<b>Grand total</b>	
<b>For discount bulk rates, call toll-free at 888/209-6554.</b>				
		<p><b>*Tax Information</b> Please include applicable sales tax. Electronic subscriptions are exempt. States that tax products and shipping and handling: CA, CO, CT, FL, GA, IL, IN, KY, LA, MA, MD, ME, MI, MN, MO, NC, NJ, NM, NV, NY, OH, OK, PA, RI, SC, TN, TX, VA, VT, WA, WI, WV. State that taxes products only: AZ. Please include \$27.00 for shipping to AK, HI, or PR.</p>		
<p><b>Your source code: N0001</b></p> <p>Name _____</p> <p>Title _____</p> <p>Organization _____</p> <p>Address _____</p> <p>City _____ State _____ ZIP _____</p> <p>Phone _____ Fax _____</p> <p><b>E-mail address</b> (Required for electronic subscriptions)</p> <p><input type="checkbox"/> Payment enclosed.    <input type="checkbox"/> Please bill me.</p> <p><input type="checkbox"/> Please bill my organization using PO # _____</p> <p><input type="checkbox"/> Charge my:    <input type="checkbox"/> AmEx    <input type="checkbox"/> MasterCard    <input type="checkbox"/> VISA    <input type="checkbox"/> Discover</p> <p>Signature _____ (Required for authorization)</p> <p>Card # _____ Expires _____ (Your credit card bill will reflect a charge to HCP Pro, the publisher of BHS.)</p>				
<p><b>Mail to: HCP Pro, P.O. Box 1168, Marblehead, MA 01945    Tel: 800/650-6787    Fax: 800/639-8511    E-mail: <a href="mailto:customerservice@hcpro.com">customerservice@hcpro.com</a>    Web: <a href="http://www.hcmarketplace.com">www.hcmarketplace.com</a></b></p>				



# HEALTHCARE SECURITY ALERT

Supplement to Briefings on Hospital Safety

## Security considerations for psychiatric patients

### ***A high-risk population requires extra preparation and effort from security staff***

A hospital ED generally brings a wide range of patient demographics, which can pose a risk to the safety of staff members.

However, an ED can become infinitely more dangerous with the addition of just one patient with behavioral health issues or mental illness, particularly if your hospital is not prepared. Further, psychiatric hospitals that cater exclusively to these patients face many challenges to ensure that staff members work in a safe environment.

The frightening circumstances of these risks came to light in October 2010 at Napa State Hospital in San Francisco, when psychiatric technician Donna Gross was strangled on the hospital grounds by Jess Willard Massey, a patient at the psychiatric facility.

A subsequent investigation by *The Los Angeles Times* discovered more than 200 attacks on staff members in the second quarter of 2010 at Napa State, increasing fourfold since the beginning of 2009, according to statistics from the California Department of Mental Health. In addition, patient attacks on one another have increased sevenfold.

The incident has forced Napa State to take a hard look at its security practices, which have been questioned by staff members through internal memos and reports dating back to June 2009, according to the *Times*. But the event has surely echoed among healthcare facilities throughout the country, says **John M. White, CPP, CHPA**, president and principal consultant for Protection Management, LLC, in Chico, CA.

"I guarantee you that facilities everywhere saw that story, heard about that story, and said, 'Okay, can that happen to us? How can we avoid that?' " White says.

Although incidents like this are largely unpredictable, he notes that spotting even the slightest warning sign can de-escalate an attack or avoid an unsafe situation, particularly in psychiatric facilities.

"I didn't read any after-action reports or anything like that, but I can tell you from things I've seen in the past, a lot of times a perfect day can go bad just because of a simple mistake, some-

one turning their back, or someone not noticing a simple warning sign," White says. "Not

**Hospitals generally aren't equipped to take care of psychiatric patients, especially for an extended period of time.**

to second-guess anyone at Napa—if you weren't there, then you really don't understand, and a lot of people will sit back and critique it later."

### **Dealing with state budget cuts**

White points to budget cuts as one of the primary hurdles for state-run psychiatric and forensic facilities, particularly in California, where the state deficit has slashed budgets on most state-run enterprises. Security is usually the first department to be downsized in this situation.

In many cases, state mental health facilities are being shut down entirely, siphoning the psychiatric patient population to general hospitals.

"The hospital, not being able to turn away any patients, they do what they can for them in the emergency department—usually screening and evaluating them—and then they spend time trying to figure out where they can place them," White says. "The security risk for mental health patients starts on the street with the public in general, and then goes into the emergency room, so the security risk starts to spread out to other people. It brings the issue right up to the forefront of

## Security considerations

< continued from p. 1

how do you deal with these people on a security level and what risks do they present to the facility.” However, hospitals generally aren’t equipped to take care of psychiatric patients, especially for an extended period of time.

Many hospitals have begun using “safe rooms,” where all the furniture and equipment is bolted to the floor and there is nothing attached to the walls, eliminating patients’ ability to harm themselves or staff members. White has heard about cases where a patient broke the legs off a table to use them as a weapon. If your hospital does not have a safe room, examination rooms should be scanned ahead of time and any dangerous or unneeded equipment should be removed.

“More and more hospitals have to hold those patients for a long period of time, trying to find facilities that will take them to help treat their mental illness,” he says. “These people can be held in the emergency room and often are held in the emergency room for hours—and sometimes more than 24 hours. That’s not a good environment to have someone in who is mentally unstable because emergency rooms can be stressful. It can be very busy, with lots of unusual noises and different smells that will sometimes aggravate someone with mental health issues.”

White suggests taking the following precautions if your hospital needs to care for a mental health patient:

- **Alert security.** Whether it’s the ambulance calling ahead or the front desk identifying patients who may be a danger to themselves or others, the security department should be involved from the moment that patient sets foot in the hospital.
- **Assign an officer to the patient.** The officer’s job is to not only protect that person from others, but also to ensure that the patient does not leave the facility if he or she is a flight risk. Some states allow officers to use physical force to detain a patient; others require the officer to use verbal de-escalating techniques or the local police department, if necessary.
- **Ensure that an officer is always in the room with a healthcare professional.** Security should be in the exam room to assist any staff members with restraining the patient or simply to offer a watchful eye.
- **Compartmentalize a dangerous situation.** If the patient begins to demonstrate aggressive behavior, isolate him or her from other patients and staff members to prevent anyone else from getting pulled in.

### Establishing a controlled environment

The key to ensuring safety is building an environment that minimizes potential dangers. This is particularly crucial in mental health facilities that sometimes host hundreds of psychiatric patients.

One crucial structural consideration for these facilities—in addition to building patient rooms free of potentially dangerous equipment—is the use of safe rooms to which staff can retreat if something goes wrong.

“Every time I come across a [mental health] facility and they don’t have one, I’m pointing that out,” White says. “It’s just like prisons. Prison guards have safe places to go to where they can lock an area down while there is an incident happening.”

Suicide is another factor to consider when treating mental health patients. On November 17, The Joint Commission issued a Sentinel Event Alert on preventing suicide among healthcare patients, particularly in the

Editorial Advisory Board	Healthcare Security Alert
	
Group Publisher: <b>Emily Sheahan</b> , <a href="mailto:esheahan@hcpro.com">esheahan@hcpro.com</a> Senior Managing Editor: <b>Jay Kumar</b> , <a href="mailto:jkumar@hcpro.com">jkumar@hcpro.com</a>	
<p><b>Russ Colling, MS, CHPA, CPP</b>  <i>Healthcare Security Consultant</i>            Colling and Kramer            Salida, CO</p> <p><b>Steven C. Dettman, BS, CHPA</b>  <i>Director, Security and Visitor Support Services</i>            Mayo Clinic Hospital            Phoenix, AZ</p> <p><b>Linda Glasson, CHPA</b>  <i>Security Consultant</i>            Suffolk, VA</p>	<p><b>Steven MacArthur</b>  <i>Safety Consultant</i>            The Greeley Company            Marblehead, MA</p> <p><b>Anthony N. Potter, CHE, CHPA-F, CPP, FAAFS</b>  <i>Market Director of Public Safety</i>            Novant Health            Winston-Salem, NC</p> <p><b>Fredrick G. Roll, MA, CHPA-F, CPP</b>  <i>President and Principal Consultant</i>            Healthcare Security Consultants, Inc.,            and Roll Enterprises, Inc.            Frederick, CO</p>

medical-surgical units and the ED. Suicide has ranked among the top five most frequently reported events since 1995, with a surprising 14.25% occurring in non-behavioral health units in the hospital, according to the alert. The Joint Commission urges hospitals to employ risk reduction strategies that include screening patients for suicidal behaviors or depression and training staff members to recognize warning signs.

### Training staff members

Officers aren't the only ones who need to undergo de-escalation training. Frontline staff need to recognize aggressive or mentally unstable behavior that can be harmful, especially if they deal with psychiatric patients on a regular basis, White says. The earlier a staff member can identify potentially dangerous behaviors, the less likely the situation will spiral out of control.

Depending on the type of facility you work in, this training can be mandated by the state or by The Joint Commission. For example, California law now requires ED staff members to undergo de-escalation training. "People are starting to understand that you can't take someone fresh out of college that has a degree in psychology and put them in [a psychiatric] environment and not teach them how to watch for signs of an explosive nature coming," White says. "They are going to get stuff like that in an educational setting, but when you get in a setting like that, you have to have more."

### Remembering the little things

Security in a healthcare facility usually means remembering to do even the simple or menial tasks to create a feeling of safety among employees. For example, escorting patients to their cars or at least stationing an officer in the parking lot during change of shift is a quick and easy task that helps staff members feel safe when they come to work.

Mentally unstable patients are unpredictable, and White says he has seen instances where mentally ill patients have come back to a facility to harass workers, even five or 10 years later. If the security department

doesn't react as if a threat is real and try to maintain a safe environment, the entire department can lose credibility in the eyes of staff members.

"It doesn't take much to devote someone to be in the parking lots at shift change to make sure all the staff that are getting off work get to their cars safely and all the people coming to work get in the building safely," White says.

### Using restraints

The use of restraints on any patient can be a contentious subject. In some cases, restraints may be required to ensure the safety of staff members or prevent patients from causing harm to themselves.

Ultimately, the decision of whether to use restraints falls to each individual hospital, says White. However, hospitals also need to consider Joint Commission requirements, specifically PC.03.05.01 through PC.03.05.19, which address the use of restraints. Those requirements include:

- Use restraints or seclusion only when doing so can be clinically justified.
- A physician or independent practitioner responsible for the care of the patient must evaluate the patient face-to-face within one hour of initiation of restraints or seclusion. A nurse or physician's assistant may conduct this evaluation as long as he or she consults with the attending physician.
- Unless a more restrictive state law exists, the physician or independent practitioner must reevaluate the use of restraints every 24 hours.

The Joint Commission instituted these changes in March 2009 to align more closely with the Centers for Medicare & Medicaid Services (CMS) *Conditions of Participation*, so you can expect the same requirements from CMS. "But for a lot of facilities, generally speaking, that's the last resort," White says. "They will try everything they can not to use restraints. But once they do, then depending on that organization, they are going to have a certain protocol they are going to have to follow." ■



## Questions of the month

# Don't overlook the little things in hospital security

*Editor's note: Healthcare Security Alert provides expert answers to your security questions. The following questions were answered by **Linda Glasson, CHPA**, security consultant in Suffolk, VA, and **Steven MacArthur**, safety consultant at The Greeley Company, a division of HCPro, Inc., in Marblehead, MA. If you have a security question for one of our experts, e-mail Senior Managing Editor Jay Kumar at [jkumar@hcpro.com](mailto:jkumar@hcpro.com).*

**Q** What are some smaller, often overlooked security measures hospitals should address?

**A Glasson:** One of the areas overlooked in the hospital is when some parts of the whole don't communicate with others. Failure to communicate with security during construction/renovation projects can lead to costly retrofits.

For example, security should be involved in decisions regarding what types of security programs/devices are needed and where—pretty basic, but there are still some facilities that don't get it. This should also include access to landscape plans so a camera doesn't get put behind a tree or, the more likely scenario, someone doesn't plant a tree in front of a recently installed camera.

Another issue to watch out for: When the security risk assessment is being prepared, the security department does not always receive information regarding an employee's aggressive behavior or drug diversions by staff. Serious consideration needs to be given to security reporting structures. Failure to do so can handcuff a department.

The security department should report to an individual who has the interest and decision-making authority at the senior leadership level. Many facilities in this budget cycle for 2011 are cutting back on training resources for nonclinical departments until they can figure out

healthcare reform and its impact. Training and appropriate staffing levels for security will be crucial in the years to come. Failure by facilities to provide for future growth in security departments does not lend itself well to the concept of "just in time."

**Q** What kind of partnership should hospital security have with local police departments?

**A MacArthur:** Some folks will have to deal with multiple local police departments, sheriff's departments, state police, state corrections officers, sometimes even the feds. It is always best to establish these relationships before they send business your way; generally, every jurisdiction has its own way of doing things, so the more you can educate yourself to their processes, the smoother your encounters will be. You could even ask to speak at their facilities (e.g., morning roll call) to help build the relationships with both the line officers and their supervisors.

There are times when you are going to have to be a pain in the tuchus, and there are times when you're going to have to function as a liaison between the clinical staff and the law enforcement folks. You do not want to be labeled as obstructionist, difficult, etc., by either side. The negotiating skills you can develop over time, but only if you have a good solid relationship from the ground up. ■

### Questions? Comments? Ideas?

Contact Senior Managing Editor  
Jay Kumar

Telephone **781/639-1872, Ext. 3144**

E-mail [jkumar@hcpro.com](mailto:jkumar@hcpro.com)