

Security management planning checklist

Editor's note: With the media spotlight and public consciousness focusing on violence in health care facilities, BOJ learned that JCAHO surveyors will likely pay close attention to hospital security in 1994. Even though the 1994 security standard (PL.1.2.1.2) is the same as the 1993 standard, look for increased scrutiny of security programs. In fact, an early draft of the 1995 Management of the Environment of Care standards reveals that security will get as much attention as safety, life safety, equipment, and utilities (see "Sneak Preview" article in last month's BOJ).

The following list covers the range of information surveyors may look for from a security management program, based on comments from a member of JCAHO's committee on health care safety. Security managers should make sure the information is part of the written security plan they submit to the safety committee-and ultimately administration and the board-for approval.

- Security mission statement.** This document should briefly describe the role security plays in the hospital's overall mission statement.
- Statement of authority.** Per Probe F in the scoring guidelines, this statement should indicate who, according to the CEO, is responsible for security.
- Relationship with outside authorities.** The JCAHO is looking to see that, when necessary, hospitals are utilizing the services of local, state, and federal authorities. This document should describe which outside authorities are used and under what circumstances.
- Trends and patterns.** This analysis is derived from security incident reports required for the safety committee. In it, the security manager should summarize any trends and patterns noticed over time. To protect against liability and discoverability of these documents, however, make sure all incidents are reported and describe only the facts about the incidents-not opinions or judgments on why they occurred.
- Manpower and training report.** The manpower report should update the current level of security staffing and electronic security support available at the hospital. It also should report on training that security personnel have received, as well as the orientation of new hires and annual training of staff who work in sensitive high-risk areas (i.e., emergency room, pediatrics, nursery, pharmacy, cashier's offices).
- Performance improvements.** This report should include data showing performance improvements achieved in the security program, such as an employee awareness program that resulted in fewer petty thefts. Cost/benefit information should be included, if available.
- Assessment of location.** In this summary, the security manager should review how the hospital's surroundings may have changed the security risk, such as demographic shifts, increases in the local community's crime rate, or rapid population growth.
- Assessment of clientele.** The security manager should summarize the security risks that accompany the population (patients, visitors, and even staff) the hospital serves.

-Assessment of services. Tied closely to the clientele assessment, this summary reviews the security risks that accompany services the hospital offers. For instance risks are greater at hospitals with a high-volume trauma center, a lock-up psychiatric unit, or an animal research lab than they are at a small, rural community hospital.

-Policies and Procedures. In addition to general security policies and procedures, the security program also should have the following policies in place.

- Access control policy
- Identification policy
- Incident response policy
- Bomb treat and disposal policy
- Hostage policy
- Infant/child abduction policy

-Goals and objectives. Based on all of the previous year's data and all the information listed above, the security director should outline reasonable security goals and objectives for the coming year.

Just the Facts... Hospital Safety and Security Infant Abduction

The Problem. Infant abduction is a growing concern in hospitals. Between 1983-1997, 171 infants (birth to age 6 months) were abducted in the U.S. Seventeen of the abductions took place in locations such as malls, offices, and parking lots; 57 took place in the home; and 97 took place in hospitals. Of the 97 hospital abductions, 55 infants were taken from their mother's rooms, 14 from the nursery, 16 from pediatrics, and 12 from the hospital grounds. At present, 5 of the 97 victims are still missing.

The Offender. As a rule, individuals who abduct infants from hospitals are non-family members having the following physical appearance and traits:

- ☛ female of "childbearing" age (12-50), overweight
- ☛ compulsive, relies on manipulation, lying, and deception
- ☛ married or living with a significant other
- ☛ indicates that she has lost a baby or is incapable of having one
- ☛ impersonates a nurse or other healthcare personnel, such as lab technicians; social workers; Women, Infant, and Children (WIC) Program staffers; photographers; etc. to gain access to the infants
- ☛ becomes familiar with healthcare personnel and even with her victim's parents
- ☛ initially visits the nursery and maternity unit at more than one hospital before the abduction
- ☛ asks staff detailed questions about procedures and the layout of the maternity unit
- ☛ uses a fire exit stairwell as her escape
- ☛ plans the abduction, but does not necessarily target a specific infant, relies on opportunity
- ☛ demonstrates ability to provide good care to the baby once the abduction occurs
- ☛ lives in the community where the abduction took place
- ☛ has no prior criminal record

Since every offender will not fit this profile, staff should always watch out for and report other unusual behaviors, such as:

- ☛ visiting repeatedly to see or hold the infants
- ☛ asking detailed questions about procedures and the building layout
- ☛ taking hospital uniforms or other means of hospital identification
- ☛ leaving the hospital on foot with an infant instead of in a wheelchair
- ☛ removing large packages from the maternity ward, particularly if cradling or talking to it
- ☛ transporting an infant in arms instead of in a bassinet

Abduction Prevention Plan. Hospital Commanders should implement a written prevention plan for infant abductions. Comprehensive Abduction Prevention Plans consist of six strategies:

Designating an Abduction Prevention Team. Commanders should designate a multidisciplinary team to develop and implement the Abduction Prevention Plan. The team's responsibilities should include assessing the healthcare facility to identify vulnerabilities, recommending/implementing physical security requirements, work practices, and employee training programs; developing emergency response plans; and auditing the program for effectiveness. At a minimum, the team should include representation from obstetric, nursery, and pediatric nurses; physicians; and security and risk management personnel.

Physical Security Assessment and Use. Physical security safeguards for abduction prevention include:

- ☛ security camera systems
- ☛ nursery and staff lounge/locker room doors equipped with self-closing, locking hardware
- ☛ alarms with time-delay locks installed on stairwell and exit doors
- ☛ electronic-asset-surveillance (EAS) detection systems

All physical security safeguards used within the healthcare facility must be constantly operational.

Establishing Work Practices for Safeguarding Infants and Children. Important work practices for safeguarding infants and children from abduction include:

- ☛ attaching matching identification bands to the infant, mother, and father or the mother's significant other (unused bands should be accounted for)
- ☛ taking footprints, color photographs, and a full physical assessment of the infant within 2 hours after birth or admission and entering the information in the infant's medical records
- ☛ using distinctive photo identification badges and uniforms in maternity, nursery, neonatal intensive care units and pediatric wards
- ☛ keeping infants in direct, line-of-site supervision at all times by a authorized staff member, the mother, or other family member designated by the mother
- ☛ transporting infants by authorized staff in a bassinet only
- ☛ verifying that the persons leaving the hospital with an infant are wearing matching identification bands
- ☛ reporting persons exhibiting behaviors of a potential abductor
- ☛ alerting other hospitals in the area of attempted abductions and of suspicious persons
- ☛ requiring parents to supervise their children at all times when in waiting rooms and outpatient clinics
- ☛ establishing an access control policy for maternity, nursery, neonatal intensive care units and pediatric wards
- ☛ keeping the mother's and infant's full name, address, and telephone number confidential

Education and Training. All staff should receive training on the Abduction Prevention Program. Key training topics that should be addressed include information on the offender profile and unusual behavior, work practices for safeguarding infants and children, and incident response and reporting. Staff working in maternity, nursery, neonatal intensive care units and pediatric wards should receive additional training on the risks, the physical security safeguards, and work practices unique to their work area(s). Staff training should be documented and the documentation should be kept for three years.

Parents should receive information on safeguarding their infant while in the healthcare facility. The National Center for Missing and Exploited Children Guidelines includes parenting techniques that should be discussed with parents upon admission and discharge and postpartum instruction.

Incident Response and Reporting. Incident response plans should include procedures for:

- ☛ using a code word, such as Code Pink or Code Stork to alert hospital personnel
- ☛ notifying security/law enforcement
- ☛ securing the facility
- ☛ searching the unit
- ☛ protecting the crime scene
- ☛ notifying other local healthcare facilities
- ☛ holding the shift in the event the incident occurs during shift changes
- ☛ dealing with the media
- ☛ caring for the parents
- ☛ caring for staff suffering from post-traumatic stress disorder

Healthcare facilities must follow the Joint Commission on Accreditation of Healthcare Facilities' Sentinel Event Policy and Procedures for reporting infant abductions.

Periodic Review and Update. The Abduction Prevention Team should assess the program for effectiveness as often as needed, but at least annually. The assessment results should be documented in the Safety Committee minutes.

References.

National Center for Missing and Exploited Children. For Healthcare Professionals: Guidelines on Prevention of and Response to Infant Abductions, 5th Edition. [Online] Available: <http://www.missingkids.com/download/infantabductions.doc>, June 1998.

Joint Commission on Accreditation of Healthcare Organizations. Sentinel Event Policy and Procedures. [Online] Available: http://www.jcaho.org/sentinel/se_poly.htm, July 18, 1998.

Wal-Mart Stores, Inc. Code Adam Operating Procedures. [Online] Available: http://www.wal-mart.com/community/codea_op.shtml, 30 December 1998.

Confront workplace violence

According to the Bureau of Labor Statistics, almost two-thirds of all reported nonfatal assaults occur in health care facilities.

Perpetrators of these assaults can range from violent patients, distraught family members, and even employees frustrated by organizational downsizing. Outpatient centers in particular are notorious for being unstable environments full of transient patient encounters.

Last March, OSHA released its workplace violence guidelines to arm health care providers to address this risk. The guidelines aren't enforceable, but OSHA can still fine facilities under its general duty clause if they don't make a "reasonable attempt to protect employees from a clear risk." New federal guidelines also expose providers to potential civil lawsuits.

Guideline recommendations

OSHA's guidelines instruct providers to begin a workplace violence program that should include a policy statement (see "Sample workplace violence policy" on p. 12), a threat assessment team, hazard assessment, hazard control and prevention, training and education, incident reporting, investigation, follow-up and evaluation, and recordkeeping.

For example, the threat assessment team should be a group that brainstorms ways to prevent violence from occurring in vulnerable areas, such as emergency rooms. It should recommend, initiate, and communicate workplace violence training and response plans to the rest of the facility.

OSHA suggests that the team should consist of a representative from senior management, operations, security, finance, legal, and human resources.

Hazard controls

To accomplish hazard control



and prevention, OSHA suggests providers design their environments to manage potential patient violence, such as arranging furniture to prevent entrapment of employees and installing lighting outdoors.

Specifically, ambulatory sites will want to follow OSHA's recommendations to protect nurse stations with enclosures that at least prevent patients from reaching behind the desk, to place curved mirrors at hallway intersections or concealed areas, and to make two

exits available in counseling or service rooms.

OSHA's other hazard control recommendations include the following:

- Use flexible staffing to meet security needs during patient escort, emergency responses, and meal times.
- Staff adequately to cover all shifts, weekends, and shift changes.
- Don't leave workers alone in situations where the potential for violence exists.
- When there is a known risk, there should be a trained response team that can provide escort service or respond to emergencies without leaving another unit's staff at risk.
- Promptly repair or replace burned-out lights and broken windows or locks.
- Regularly test and maintain alarm systems, including personal alarm devices, batteries, and any other mechanical device used for safety.
- Work with local police to establish response mechanisms and report all violent incidents to the police.
- Have lockable bathrooms available for staff separate from patient rest rooms.
- Install alarms or panic buttons in high-risk areas.
- Control workloads so employ-

ees are not too tired to identify potentially violent situations.

Warning signs

To be able to spot any potential for violence, employees need security education, says

Anthony Potter, director of public safety for Emory University System of Health Care in Atlanta. Education alone reduces the chance of violence because staff are then able to recognize the warning signs of an employee or patient who is at risk of becoming violent, he explains.

According to the International Association of Chiefs of Police, Alexandria, VA, and The Kenwood Group in San Francisco, an employee at risk for violence often

- makes veiled or direct verbal or written threats,
- intimidates others either physically or verbally,
- is fascinated with weaponry or violent acts,
- exhibits paranoid behavior,
- drastically changes his or her belief system,
- exhibits moral righteousness about his or her perception that the facility isn't following its own policies and procedures,
- is unable to handle criticism about his or her job performance,
- expresses extreme despera-

tion over personal problems,

- has a history of violent behavior,
- is fascinated with other workplace violence incidents,
- disregards other employees' safety,
- becomes obsessively involved with his or her job,
- takes up supervisor's time with performance problems,
- steals or sabotages projects or equipment, or
- becomes romantically obsessed with a co-worker who doesn't share his or her interest.

Action points

To stop these behaviors before they begin, Potter recommends that facilities write a policy prohibiting concealed

weapons and provide a gun locker for employees who bring weapons to work. He also feels providers should conduct a criminal and driving history check on job candidates to assess their characters.

In addition to having a workplace violence policy, hazard controls, and educating staff about the warning signs of violence, Potter urges providers to

- set up a violence response plan that is accessible to employees,
- respond appropriately (see "Do's and Don'ts," p. 13), and
- document everything to comply with accreditors and OSHA. ♦

Editor's note: OSHA's complete workplace guidelines can be read on-line at <http://www.osha.gov>.

Related accreditation standards

No accreditation standards specifically refer to workplace violence. But ones that are related to OSHA's workplace violence guidelines are the Joint Commission on Accreditation of Healthcare Organization's (JCAHO) EC.1.4 standard in its *1996 Comprehensive Accreditation Manual for Ambulatory Care*, and the Accreditation Association for Ambulatory Health Care's occupational health services standards in its *1996/1997 Accreditation Handbook*.

The AAAHC's occupational health services chapter simply states that a ambulatory site's occupational health services must be provided in compliance with OSHA. The JCAHO's EC.1.4, however, is more specific; it outlines what elements a security plan should have, such as emergency procedures for civil disturbances and security incidents that are evaluated yearly. ♦

Sample workplace violence policy

Our establishment, [Employer name], is concerned about and committed to our employees' safety and health. We refuse to tolerate violence in the workplace and will make every effort to prevent violent incidents from occurring by implementing a Workplace Violence Prevention Program (WVPP). We will provide adequate authority and budgetary resources to responsible parties so that our goals and responsibilities can be met.

All managers and supervisors are responsible for implementing and maintaining our WVPP. We encourage employee participation in designing and implementing the program. We require prompt and accurate reporting of all violent incidents whether or not physical injury has occurred. We will not discriminate against victims of workplace violence.

A copy of this policy and our WVPP is readily available to all employees from each manager and supervisor.

Our program ensures that all employees, including supervisors and managers, adhere to work practices that are designed to make the workplace more secure and do not engage in verbal threats or physical actions that create a security hazard for others in the workplace.

All employees, including managers and supervisors, are responsible for using safe work practices, for following all directives, policies and procedures, and for assisting in maintaining a safe and secure environment.

The management of our establishment is responsible for ensuring that all safety and health policies and procedures involving workplace security are clearly communicated and understood by all employees. Managers and supervisors are expected to enforce the rules fairly and uniformly.

Source: Occupational Safety and Health Administration, Washington, DC.

Do's and don'ts in a potentially violent situation

Anthony Potter, director of Atlanta's Emory University System of Health Care, suggests the following Do's and Don'ts when attempting to de-escalate a potentially violent situation.

1. Project calmness—move and speak slowly, quietly, and confidently.

Don't use communication styles that produce hostility—apathy, brush-off, coldness, condescension, robotism, going strictly by the rules, or giving the runaround.

2. Be an empathetic listener—encourage the person to talk, and listen patiently.

Don't reject all of his or her demands at the start.

3. Focus your attention on the person to let him or her know you are interested in what he or she is saying.

Don't pose in challenging stances—standing directly opposite, hands on hips, arms crossed, in physical contact, pointing fingers, or with long periods of fixed attention.

4. Maintain a relaxed yet attentive posture, and position yourself at a right angle rather than directly in front of the person.

Don't make sudden movements that can be interpreted as threatening.

5. Acknowledge the person's feelings. Indicate that you can see he or she is upset.

Don't challenge, threaten, or dare the individual; don't belittle the person or make him or her feel foolish.

Don't criticize or act impatiently toward the agitated individual.

6. Ask for small, specific favors such as asking the person to move to a quieter area (preferably where there are no objects that can be used as weapons).

Don't attempt to bargain with a threatening person.

7. Establish ground rules if unreasonable behavior persists. Calmly describe the consequences of any violent behavior.

Don't treat the situation as trivial.

8. Use delaying tactics to give the person time to calm down. For example, offer a drink of water (of course, from a paper cup).

9. Be reassuring and point out choices. Break big problems into smaller, more manageable ones.

Don't try to impart a lot of technical or complicated information when emotions are running high.

10. Accept criticisms in a positive way. When a complaint might be true, use statements like "You're probably right" or "It was my fault." If criticism seems unwarranted, ask clarifying questions.

Don't take sides or agree with distortions.

11. Ask for his or her recommendations. Repeat back to him what you feel he or she is requesting of you.

Don't make false statements or promises you cannot keep.

12. Position yourself so that you have immediate access to an exit.

Don't invade the individual's personal space. A good distance is three to six feet away.

13. Be aware of anything in the room that can be used as a weapon.

ARCHITECTURAL RECORD

news

search

go

[Return to WTC coverage](#) | [E-Mail This Article](#)

news

daily news
from the field

projects

project portfolio
building types study
record houses
lighting

archrecord2

for the emerging
architect

features

interviews
bw/ar awards

departments

digital practice
building science/
continuing ed.
green architect
editorial
letters
events

about record

magazine index
subscribe
how to submit
advertise
editorial calendar
privacy policy
contact us
site map

the AIA

join the AIA
www.aia.org
contract documents

services

bookstore
recruitment
reader service
professional
directories

home

Record News: Special Report

From *Architectural Record*, January 2002

Symposium speakers insist on freedom without fortresses

By John E. Czarnecki, Assoc. AIA

Buildings in the United States, especially public buildings, cannot be built as insular fortresses that are unwelcoming to the public. That was the message of speakers, including the Honorable Daniel Patrick Moynihan, former U.S. senator from New York, in a symposium "Freedom Without Fortresses? Shaping the New Secure Environment," at the National Building Museum in Washington, D.C., on November 27. The symposium, cosponsored by ARCHITECTURAL RECORD, the American Institute of Architects, the Urban Land Institute, and RTKL, explored the impact of the September 11 attacks on the built environment.

Moderated by Robert Ivy, FAIA, editor in chief of ARCHITECTURAL RECORD, the panel addressed questions related to urban planning, psychology, and public spaces. Harold L. Adams, FAIA, RIBA, JIA, chair of RTKL, introduced Moynihan, who said public buildings must have free and open access. "Architecture is inescapably a political art and it reports faithfully for ages to come what the political values of a particular age were," Moynihan said. "Surely ours must be openness and fearlessness in the face of those who hide in the darkness. A precaution, yes. Sequester, no."

Other speakers included architect and planner Jonathan Barnett, FAIA, AICP; Richard Farson, president, Western Behavioral Sciences Institute; and Jeri Thomson, secretary of the U.S. Senate.

Photos: © F.T. Eyre

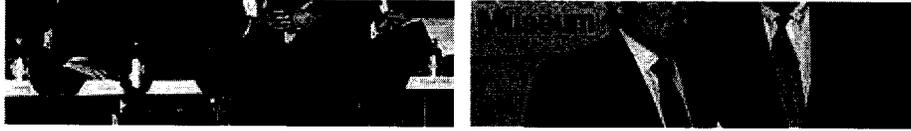


[Online WTC coverage index](#)

Special Magazine coverage:

- [Symposium speakers insist on freedom without fortresses](#)
- [Panelists: Despite terrorist attack, the skyscraper is here to stay](#)
- [First downtown N.Y.C. building completed post 9/11 opens](#)





Symposium participants (from left) Daniel Patrick Moynihan, Richard Farson, Robert Ivy, FAIA, and Harold L. Adams, FAIA, with Farson.

Farson, a psychologist, spoke of the psychology of security and noted 10 paradoxes and unintended consequences of security measures:

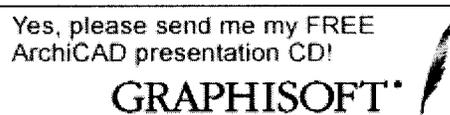
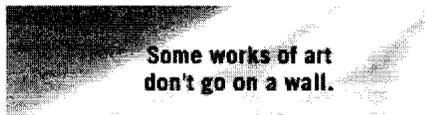
1. *Security is an illusory concept. Complete security, of course, is impossible. We cannot protect against what we cannot imagine.*
2. *Since complete security is impossible, can we be rational about it? That is, if all we can do is improve the odds, let's look at the odds. What are the odds that anyone will be on a hijacked airplane this year? Well if there's a hijacking this year and if there is a hijacking every day this year and you flew every day this year, that your odds would be 20,000 to one.*
3. *The paradox of national success is that our very strength makes us vulnerable. Our power, our wealth, our standard of living, our influence, and a complex target-rich environment, as they say. We cannot become invulnerable because it is not our weaknesses but our strengths that make us vulnerable.*
4. *The emphasis on security makes people suspicious and afraid of each other and that's very dangerous. Nothing makes people more secure than a sense of community and when people are made suspicious of each other, you lose community.*
5. *We play a dangerous security game with terrorists. Every time we take a measure in, say, airline security, the terrorists escalate. And so we are back and forth with an escalating process and the outcome of it, believe it or not, is that as we increase this there is greater death and destruction in recent years than there was when we began this.*
6. *We believe that individuals are fragile and institutions and governments and nations are strong. It's the other way around, that individuals are very strong. It's very difficult to damage an individual, but relationships, communities, organizations, institutions, and governments are very fragile. And we've seen them collapse.*
7. *With concurrent technology we can build a structure that can withstand just about anything a terrorist can do. The trouble is nobody could afford to build it and nobody would want to live or work in it. Architects need to be able to say no to requests for buildings that will make life worse. A profession, when it's at its best, can say no to things that it knows it shouldn't do. It's important that architecture operate as a responsible profession, not just as a market-driven business and remember that there is a giant security industry and now architecture is part of that.*
8. *There are buildings that need to be high-security buildings. I believe embassies, military installations, and certainly other buildings need it. But I think by and large we need to be very parsimonious in this and introduce only security measures that are quickly accomplished, not intrusive, particularly if they're invisible that's better. Low cost, demonstrably effective.*

9. *Architects, without their knowing it, sometimes design organizations. They don't just reflect organizations, don't just accommodate organizations, they actually design them. The kind of spaces that architects design make certain that certain kinds of relationships take place. So we should move away from megastructures to designing smaller-scale organizations, schools that are not 4,000 but 400, prisons that are not 10,000 but 18 or 20 people because we know from psychology that you can rehabilitate a prisoner if there are only 18 or 20 people.*

10. *Architecture is potentially more important in building a great society than education, or medicine or any other profession. The reason is that design situations and situations are what determine behavior. You're going to have to have leadership in this. And you're going to have to build more wonderful airy spaces where people are healthier, less dysfunctional, more productive, more creative, and you know how to do this. Adopting a heavy security orientation is an impediment to architecture in the public interest.*

Brief responses to the presenters were offered by Angela R. Cavaluzzi, New York City Planning Commissioner, and Carol Blonar, vice president and director of facilities management for T.Rowe Price Group. Technical experts on the panel were Thomas J. Rittenhouse III, principal and blast specialist with Weidlinger Associates, and David V. Thompson, AIA, vice president with RTKL Associates.

[Return to WTC coverage](#) | [Return to news headlines](#)



[News](#) | [Projects](#) | [Digital Architect](#) | [Green Architect](#) | [Advertisers & Products](#) | [Editorial](#) | [Jobs](#)
[Letters](#) | [Record Houses](#) | [Events](#) | [Interviews](#) | [Continuing Ed](#) | [About Record](#) | [Home](#) | [top](#)