Civil unrest in Ferguson, Missouri: security’s role in preparing for man-made surge events
Richard C. Bartram

Surviving the first five to seven minutes!
Jeff Putnam, CPP and William Losefsky, CHPA

How to avoid having to “run-hide-fight”
James R. Sawyer, CHPA, CPP

Threat Assessment Teams
Lisa Pryse Terry, CHPA, CPP

Emergency codes: a study of hospital attitudes and practices
Alexandra Mapp, MPH; Jennifer Goldsack, MBA, MChem, MA, MS; Leslie Carandang; James W. Buehler, MD; and Seema S. Sonnad, PhD

Securing a healthcare facility during street celebrations
Paul Grant

Secure partnership: ENA, IAHSS leaders agree on need for continued team-up
Amy Carpenter Aquino

Violence in healthcare—one nursing student’s perspective
Michael S. D’Angelo, CPP

Improving staff safety and the patient experience through redesign of security’s role in the emergency department
Drew Neckar, CHPA, CPP

Preventing child sexual abuse in youth-serving organizations
Norman D. Bates, Esq., Christine Army, MA

To treat and cure them, you must first keep them safe
Dr. James D. Blair, FACHE

Blue ribbon panel hears how to respond to biological and chemical threats
Anthony Kimery

Budget reductions vs loss of security training
John M. White CHPA, CPP

An alternative view in the development of healthcare security metrics
Anthony Luizzo, PhD, CFE, CST, PI (ret. NYPD) and Bernard J. Scaglione, CPP, CHPA, CHSP

Beating plowshares into shields: forging best practices into useful validation tools
Christopher E. Komst

Security staff turnover: a positive and a negative
Russell Colling CHPA, CPP

Why would I want to work for you?
Dan Beaver, CHPA

Seven steps for starting and building an effective hospital security K9 program
Mike Angeline, HEM, CHSP, CHCM, CAM
## Table of Contents

<table>
<thead>
<tr>
<th>ARTICLE</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Civil unrest in Ferguson, Missouri: security’s role in preparing for</td>
<td>1</td>
</tr>
<tr>
<td>man-made surge events...</td>
<td></td>
</tr>
<tr>
<td>Richard C. Bartram</td>
<td></td>
</tr>
<tr>
<td>Surviving the first five to seven minutes!</td>
<td>10</td>
</tr>
<tr>
<td>Jeff Putnam, CPP and William Losefsky, CHPA</td>
<td></td>
</tr>
<tr>
<td>How to avoid having to “run - hide - fight”</td>
<td>15</td>
</tr>
<tr>
<td>James R. Sawyer, CHPA, CPP</td>
<td></td>
</tr>
<tr>
<td>Threat Assessment Teams</td>
<td>23</td>
</tr>
<tr>
<td>Lisa Pryse Terry, CHPA, CPP</td>
<td></td>
</tr>
<tr>
<td>Emergency codes: a study of hospital attitudes and practices............</td>
<td>36</td>
</tr>
<tr>
<td>Alexandra Mapp MPH, Jennifer Goldsack, MBA, MChem, MA, MS, Leslie Carandang, James W. Buehler MD, and Seema S. Sonnad PhD</td>
<td></td>
</tr>
<tr>
<td>Securing a healthcare facility during street celebrations...............</td>
<td>48</td>
</tr>
<tr>
<td>Paul Grant</td>
<td></td>
</tr>
<tr>
<td>Secure partnership: ENA, IAHSS leaders agree on need for</td>
<td>52</td>
</tr>
<tr>
<td>continued team-up</td>
<td></td>
</tr>
<tr>
<td>Amy Carpenter Aquino</td>
<td></td>
</tr>
<tr>
<td>Violence in healthcare--one nursing student’s perspective ...............</td>
<td>56</td>
</tr>
<tr>
<td>Michael S. D’Angelo, CPP</td>
<td></td>
</tr>
<tr>
<td>ARTICLE</td>
<td>PAGE</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Improving staff safety and the patient experience through redesign of security's role in the emergency department</td>
<td>62</td>
</tr>
<tr>
<td><em>Drew Neckar, CHPA, CPP</em></td>
<td></td>
</tr>
<tr>
<td>Preventing child sexual abuse in youth-serving organizations</td>
<td>71</td>
</tr>
<tr>
<td><em>Norman D. Bates, Esq., Christine Army, MA</em></td>
<td></td>
</tr>
<tr>
<td>To treat and cure them, you must first keep them safe</td>
<td>80</td>
</tr>
<tr>
<td><em>Dr. James D. Blair, FACHE</em></td>
<td></td>
</tr>
<tr>
<td>Blue ribbon panel hears how to respond to biological and chemical threats</td>
<td>85</td>
</tr>
<tr>
<td><em>Anthony Kimery</em></td>
<td></td>
</tr>
<tr>
<td>Budget reductions vs. loss of security training</td>
<td>91</td>
</tr>
<tr>
<td><em>John M. White, CHPA, CPP</em></td>
<td></td>
</tr>
<tr>
<td>An alternative view in the development of healthcare security metrics</td>
<td>98</td>
</tr>
<tr>
<td><em>Anthony Luizzo, PhD, CFE, CST, PI (ret. NYPD)</em></td>
<td></td>
</tr>
<tr>
<td>and Bernard J. Scaglione, CPP, CHPA, CHSP</td>
<td></td>
</tr>
<tr>
<td>Beating plowshares into shields: forging best practices into useful validation tools</td>
<td>105</td>
</tr>
<tr>
<td><em>Christopher E. Komst</em></td>
<td></td>
</tr>
<tr>
<td>Why would I want to work for you?</td>
<td>110</td>
</tr>
<tr>
<td><em>Dan Beaver, CHPA</em></td>
<td></td>
</tr>
<tr>
<td>Security staff turnover: a positive and a negative</td>
<td>115</td>
</tr>
<tr>
<td><em>Russell Colling, CHPA, CPP</em></td>
<td></td>
</tr>
<tr>
<td>Seven steps for starting and building an effective hospital security K9 Program</td>
<td>119</td>
</tr>
<tr>
<td><em>Mike Angeline HEM, CHSP, CHCM, CAM</em></td>
<td></td>
</tr>
</tbody>
</table>
The Journal of Healthcare Protection Management, a publication of the International Association for Healthcare Security & Safety, is published two times a year by IAHSS—in the Winter and the Summer. A copy of each issue is distributed free to current paid-up members of IAHSS.

Digital copies of recent issues can be accessed by members in the Archives Files of the IAHSS website.

The Journal has been selected for citation in the National Library of Medicine's Health Planning and Administration database, which is now available online to over 2,000 organizations in the U.S., as well as to many overseas users.

SUBSCRIPTION RATES
For non-members, the price per issue is $13; the subscription price (two issues) is $25. The above rates apply only to the US. Outside US, add $10 per issue or $20 per year—US dollars only.

TO OBTAIN COPIES
IAHSS members will receive their copies automatically upon publication. Non-members who wish to purchase individual issues to subscriber at the two-issue rate should send the appropriate amount in US dollars to: Subscription Department, Rusting Publications, 51 Great Neck Road, Great Neck, NY 11021.

EDITORIAL CORRESPONDENCE
Please address all letters of manuscript submissions to: Rusting Publications, 51 Great Neck Road, Great Neck, NY 11021, or phone 516-467-4472.
E-mail: robertrusting@gmail.com

ADVERTISING SALES

CHANGE OF ADDRESS
IAHSS members should send all change of address information to the Association at: P.O. Box 5038, Glendale Heights, IL 60139.

Non-member subscribers should send change of address information to: Rusting Publications, 51 Great Neck Road, Great Neck, NY 11021.
CALL FOR ARTICLES

This is a call for articles for the forthcoming Winter issue (Volume 32, Number 1) of the Journal of Healthcare Protection Management. The issues that have been published to date have won considerable acclaim in the industry for their positive contributions to the fields of healthcare security and safety. In addition to the membership of IAHSS, subscribers include health facilities and libraries in a number of foreign countries.

We are interested in articles of virtually any size (from 1,000-5,000 words) that will benefit your colleagues in such areas as:

- access control
- bioterrorism
- budgeting
- productivity
- computer applications
- security liability
- training security officers
- dealing with violent crime
- crime prevention programs
- safety issues in healthcare
- coping with budget cuts
- employing technical equipment (i.e., CCTV, alarm systems)
- emergency drills
- disaster response
- ID theft
- forensic patients
- proprietary vs. contract
- reducing drug diversion
- working with police/fire departments
- hostage incidents
- reducing employee theft
- expanding security's role
- infant kidnapping
- HazCom regulations
- winning management help
- staffing
- research studies, surveys
- employee screening
- homeland security
- workplace violence

You do not have to be a member of IAHSS to author an article in the journal. Nor do you have to be a professional writer. A straightforward account of how you, your department, or your healthcare institution have successfully carried out programs in the above or other subject areas will be welcome. Camera-ready illustrative material (i.e., charts, tables, graphs) will also be considered. If you would like to submit or discuss a possible article, please write to: Rusting Publications, 51 Great Neck Road, Great Neck, NY 11021. E-Mail: robertrusting@gmail.com
Civil unrest in Ferguson, Missouri: security’s role in preparing for man-made surge events

Richard C. Bartram

A first-hand account of the role of healthcare security in preparing for and responding to protests, demonstrations, and violence from man-made surge events such as the extended civil unrest in Ferguson, Missouri, is presented by the author, who also provides guidance for other healthcare professionals facing similar situations.

Hospital preparedness for riot emergencies requires the hospital’s disaster plan be put into effect at the onset of any civil disturbance that may result in a riot.

In the event a riot would develop, other steps would be taken to effectively safeguard patients, staff, visitors and hospital property. This would consist primarily of maintaining close coordination and communication with area law enforcement, fire department personnel and hospital/clinic leadership. While this policy provides guidance at the hospital itself, there also was a need for protecting our Mercy clinics and our home health care patients who reside within the confines of a civil unrest area, away from the campus.

That happened to be the scenario experienced in 2014 from August to December in Ferguson, Missouri, a suburb of St. Louis.
with a population of 21,000, 17 miles away from the Mercy St. Louis Hospital campus. Protests against police, which sometimes led to considerable violence, received continuous national and international media coverage. Similar actions of civil unrest have occurred since then following protests against police in Baltimore and Cleveland

CIRCUMSTANCES AND EVENTS LEADING UP TO THE CIVIL UNREST

The following is a synopsis of the circumstances and events which led up to the civil unrest in Ferguson. These are facts from the original police/federal investigation, which have been made available to the public. These statements are no way the opinion of Mercy St. Louis Hospital or the Mercy Health Care System.

On Saturday August 9th, 2014, at 11:51 a.m., the Ferguson police dispatcher announced a robbery at a convenience store in their venue. A description of the subject responsible for the robbery was placed over their radio system, adding the location the subject was last seen traveling.

At 12:01 p.m. Ferguson police officer Darren Wilson while on routine patrol, observes a subject jaywalking down the center of the street. While no one knows exactly what transpired during these few moments, witnesses provide testimony that the suspect and the police officer struggled and fought inside of the officer’s patrol car. Subsequently, the suspect, now identified as Michael Brown, is shot to death as a result of the encounter.

On Sunday August 10th at 10 a.m.—St. Louis County Police Chief Jon Belmar, now in charge of this shooting investigation, states in a news conference, that the subject killed, one Michael Brown, 18 years of age, was unarmed at the time of his encounter with Ferguson Police Officer Darren. It is believed Michel Brown was the person involved in the strong-arm robbery of the convenience store.

Chief Belmar announces that suspect Michael Brown physically assaulted the police officer, and during a struggle, which ensued between the two, Michael Brown attempted to wrestle the gun away from the officer. As a result, one shot was fired inside the police car, followed by other gunshots outside of the car.
Later this same night, a candle-light vigil to honor Michael Brown turns violent. More than a dozen businesses in Ferguson are vandalized or looted; some of which were burned. More than thirty people are arrested and two police officers suffered injuries.

On Monday August 11th, the first day of school is cancelled in Jennings—a community adjacent to Ferguson—for safety of students who could be walking into violence stemming from the civil unrest. Ferguson police and city leaders say a number of death threats to the police force have been received in relation to the fatal shooting. Hundreds gather outside the Ferguson Police Department to demand justice for Brown's death. Police arrest at least seven people.

The Federal Bureau of Investigation announces its agency will perform a parallel investigation into the shooting of Michael Brown. Concurrently, the St. Louis County Police Department announces it will release the name of the officer, who is accused of shooting Michael Brown.

This same afternoon, the parents and attorney of Michael Brown hold a press conference, where they ask for a stop to all the violence; demanding justice for their son. That night, several people gather again on West Florissant Avenue in Ferguson in a planned peaceful protest. However, the crowd turns unruly, causing the police to use tear gas to disperse them and gain order.

August 12th 10 a.m.—Protesters gather at St. Louis County Police Department headquarters in Clayton, Missouri, where Mercy has physician offices. Reverend Al Sharpton arrives in St. Louis to demand justice in the fatal shooting of Michael Brown. Once night falls, the protests in Clayton and Ferguson, again turn to violence.

August 18th 2 a.m.—Governor Nixon orders the National Guard into Ferguson after protesters shot at police, threw Molotov cocktails at officers, looted local businesses and carried out a "coordinated attempt" to block roads and overrun the police's command center, Nixon's office said in a statement. Ferguson-Florissant School District cancels school for the rest of the week; amid safety concerns for students.

3:30 p.m.—President Obama announces he is dispatching At-
torney General Eric Holder to monitor the unrest in Ferguson. Obama called on people to address "the gulf" that exists between minorities and law enforcement, but must do so with respect for all sides.

August 20th 12 a.m.--Though protests were less confrontational Tuesday night into Wednesday morning than in recent days, 47 people were arrested and threats were made to kill a police officer, said Captain Ron Johnson of the Missouri State Highway Patrol.

A grand jury began investigating whether Ferguson police officer Darren Wilson should be criminally charged for the death of Michael Brown.

Friends, family and strangers say goodbye to Michael Brown at a funeral at the Friendly Temple Missionary Baptist Church.

September 16th--Ferguson Police Officer Darren Wilson testifies before a grand jury, which is reviewing evidence in Michael Brown's death, to determine whether Officer Wilson should face criminal charges.

October 10th--"Ferguson October," a four day peaceful protest with planned civil disobedience, begins, while police investigate the shooting deaths of Michael Brown and a second black teenager in the area, killed by police--Vonderrit Myers Jr.--after an exchange of gunfire.

November 11th--Missouri Governor Jay Nixon said he will move the National Guard to respond to any unrest that erupts after the grand jury delivers its decision. "Violence will not be tolerated," he said.

PREPARING FOR THE AFTERMATH OF THE GRAND JURY DECISION

To meet the need for additional security, Mercy St. Louis reached out to other hospitals within the Mercy Health Care system for resources--both manpower and equipment. Mercy Springfield and Mercy Oklahoma were gracious enough to volunteer security personnel and vehicles, during this time of need.

In addition, a referral was made to Champion National Security, based out of Richardson, Texas, with a local presence in St. Louis. Champion was contacted and two representatives responded to work out the details for manpower. A contract was drawn up with the company agreeing to supply a certain number of secu-
rity officers to the needed locations; coupling with existing Mercy security personnel to supplement an available security presence.

At the same time information was delivered to all the facilities about the situation. This included:

“Picketing is legal, as are rallies on public property. Most of the rallies include leafleting by several outside groups. Security’s response must be proportionate to the threat.

“Police will not respond to a facility simply because people are picketing or assembling on public property, which is legal. You will need to contact the police if patient access to care in your facility is blocked by people occupying your building or parking areas.

“Part of our situational awareness is identifying ‘hot spots’. Please be sure you contact security when you call the police for illegal activity at any of your facilities. Security also needs to be contacted if picketing or other legal activity--which does not require police intervention--occurs at your facility.

“Protection of your co-workers during home visits is also covered in our plan. Prior actions of completing home visits prior to noon is effective and will continue. If co-workers feels unsafe in entering a neighborhood, they should drive to a safe location and call you. You can then reschedule that visit or complete the visit by telephone, if appropriate. This is the plan we implemented earlier. Contact me on my cell phone, listed in the signature line, for additional concerns or clarification.”

TARGETS FOR POTENTIAL ACTIONS

Below is a partial of the published list of potential St. Louis area targets, or Potential Action Locations as referred to by the Ferguson Protest group:

- Robert McCulloch’s office
- St. Louis County Justice Center
- Judge Maura McShane’s courtroom
- St. Louis County Police Department
- Governor Nixon’s Office (Wainwright Building)
- St. Louis City Justice Center
- St. Louis City Police Department
- Mayor Slay & Colonel Jon Belmar
- Senators Blunt &
McCaskill
• Lambert International Airport
• Gateway Arch
• St. Louis Galleria
• Plaza Frontenac
• Ritz Carlton
• Boeing
• St. Louis University Hospital
• SSM Cardinal Glennon Children’s Medical Center
• SSM St. Mary’s Health Center
• Barnes Jewish Hospital
• St. Alexius Hospital
• Kindred Hospital [Within Mercy St. Louis]
• Southwest Medical Center

It was also emphasized that the Ferguson Mike Brown protesters were not ruling out violence or looting. "Rioting and looting are the tools of those without a voice. The rioting and looting, while I didn't participate in it, was necessary. Without it we would not be standing here today." (Rockit Ali, a 22-year-old demonstration organizer.)

THE GRAND JURY DECISION AND CROWD RESPONSE: THE FIRST NIGHT

November 24th--Clayton, Missouri. A St. Louis County grand jury has brought no criminal charges against Darren Wilson, a white police officer who fatally shot Michael Brown, an unarmed African-American teenager, more than three months ago in nearby Ferguson. The decision by the grand jury of nine whites and three blacks was announced Monday night by the St. Louis County prosecutor, Robert P. McCulloch, at a news conference.

Word of the decision set off a new wave of anger among hundreds who had gathered outside the Ferguson Police Department. Police officers in riot gear stood in a line as demonstrators chanted and threw signs and other objects toward them as the news spread. In downtown Ferguson, the sound of breaking glass could be heard as crowds ran through the streets.

As the night went on, the situation grew more intense and chaotic in several locations around the region. Bottles and rocks were thrown at officers, and windows of businesses were smashed. Several police cars were burned; buildings, including a Walgreens, a meat market and a storage facility, were set on fire.
and looting was reported in several businesses. Gunshots could be heard along the streets of Ferguson, and law enforcement authorities deployed smoke and gas to control the crowds.

MAINTAINING SECURITY AND COMMUNICATIONS AT VARIOUS MERCY LOCATIONS

On the evening of the 24th and for several nights following, heightened security was provided at several locations—Mercy Corporate headquarters, six clinic practices in close proximity to the Ferguson/Florissant area and others in downtown Clayton—where the County seat is located. The clinics operated on an as needed time schedule, cutting their hours short, notifying patients of the change and availability. While there were incidents throughout the community, there was little activity reported at any of the Mercy St. Louis locations. It was eerily quiet.

A blow to our providing additional security manpower to meet these additional needs occurred when Champion executives informed us they were backing out of their agreement because they had been ordered to be protective of their current clients in St. Louis and not service any new clients. This denial of service forced us to keep our security personnel on 12-hour shifts for an extended period.

Communications. Mercy St. Louis security leadership remained at the hospital around the clock, updating senior leadership on a regular basis. To do this effectively it was essential to stay in contact with the Police Command Center (as Mercy Media Relations did) and keep updated contact information with local and major police departments. For example, the Police Command Center contacted Mercy St. Louis security, advising there was no loss of life and no major injuries as a result of the protests during the night. However, considerable property damage was incurred to selected communities.

The National Guard. We received a late notification that the National Guard—four officers—three armed for patrol and relief; one medic, will be stationed in their Emergency Department. They are there to assist security if the need arise. Security requested a blanket email be sent to all co-
workers, advising the National Guard is on campus and may be seen inside the building for meals and breaks. It was important to let staff know why there was a National Guard presence on campus.

**Responding to a bomb threat.** There was a high probability for bomb threat phone calls during the civil unrest being experienced by our community. The intent here is to draw local law enforcement to a single location, weakening our ability to respond elsewhere. This allows unpatrolled areas, which sometimes afford the opportunities to commit the kind of actions we experienced last night, throughout the community.

**Protestors As Patients.** Mercy St Louis had two protestors come in as patients: one on their own accord and one as a fit for confinement for the St. Louis County police department. Neither had significant injuries, both were treated and discharged.

**Security Personnel.** Security leadership put an e-mail out to its personnel working the 12-hour shifts, advising officers to make arrangements for elderly family members, pets, medications taken and family conveyance needs. The 12-hour shifts not only placed a burden on the officers, but the family members as well. Security leadership was inundated with calls from family members or significant others, wanting to know the duration of the extended shifts, could their spouse/loved one just be home for dinner one evening or attend special event occurrences within the family.

**Co-workers Concerns.** Multiple phone calls were fielded by security dispatch and the voice service’s department from co-workers who are concerned about their safety in coming to and going from the campus. Senior leadership sends e-mails and updates to other hospital leaders on what is being done to protect the campus and the co-workers.

**Security in the days following the verdict.** Each night police and demonstrator confrontations dwindle. The looting, burning of buildings and melees lessen as the week continues. By Wednesday, November 26th the community returns to a somewhat normal operations. Thursday morning, the Springfield and Oklahoma officers are returned to their home base, in time to celebrate the
Thanksgiving holiday. The National Guard remains on campus, however, and Mercy St. Louis security remains on 12-hour shifts. On Monday, December 1st, Mercy St. Louis returns to normal eight-hour shift. It is estimated Mercy St. Louis expended in excess of $27,750 for security overtime, travel, housing and meals.

LESSONS LEARNED

Our experiences dealing with the civil unrest in Ferguson, we believe, can be utilized by health systems in markets large or small.

1. An Emergency Preparedness Plan is essential for man-made surge events for both hospital campuses and outside facilities. It is essential that all facilities understand the plan.

2. Communication is critical with law enforcement, management team and staff members, outside facilities and other hospitals.

3. It is important to keep updated contact information with your local and major police departments.

4. If you feel you will need assistance outside of your organization—PLAN EARLY.

5. Then have a Back Up Plan in case assistance doesn’t materialize (i.e. the Champion National Security withdrawal).

6. If there is a National Guard presence on campus, let staff know.

7. Ensure you have a good understanding with your finance VP.

One thing I cannot emphasize enough is the need to establish a relationship with the local law enforcement in which your facility resides in advance of any crisis. I came to Mercy St. Louis after thirty plus years in law enforcement during which time I was part of a supervisory team that included three hospitals in my area. One thing I learned from this was that the only time we heard from them was when they needed something. That alone clued me in on what “not” to do here at Mercy. Shortly after arriving, I included local police department and other law enforcement agencies in hospital needs and events. I insured their leadership were invited to not only important meetings, but gala events—i.e. celebrations, dances, parties, etc.—mostly conducted by the hospital Foundation department. When we held situational planning for events, such as an active shooter or hostage situations, we invited the police hierarchy and even Federal personnel. Police sub-stations were set up in the hospital for the officer on patrol to come in to use the phone, computer, or just let us know who he/she was. We embraced the police department and it paid off.
The first five to seven minutes!

Jeff Putnam, CPP and William Losefsky, CHPA

The time interval between the arrival of an active shooter and the response of local police can produce a traumatic number of casualties and injuries. In this article, the authors spell out the passive and active steps which employees can be trained to take to save their lives in this critical period.

If you are a Hospital Security Director or Manager, you more than likely already have an active shooter plan in place. The adage of “RUN/HIDE/FIGHT,” we believe, is still critical to a good active shooter plan. However, most plans fall short in that they weigh heavily on waiting for local law enforcement to respond to neutralize the shooter(s). This philosophy is understandable, but an “outstanding plan” will address what to do during the first 5-7 minutes—that critical period between when the first shots are fired and when law enforcement officers can actually respond to take out the threat.

YOUR FIRST STEP: HAVE A COMMUNICATIONS SYSTEM IN PLACE

In a 2012 Annals of Emergency Medicine study, researchers found 154 hospital shootings from 2000 to 2011, occurring in 40 states, with 235 injured or fatalities. Emergency Departments were listed as the most common site of attacks (29%), followed by
the parking lot (23%) and patient room (19%). During an Active Shooter situation, the Security Practitioner’s goal is to prevent or reduce the likelihood of injury or death. The average law enforcement response time for an Active Shooter Event (ASE) is 5-7 minutes, depending on your geographical location, department staffing and other associated variables.

Training your staff on and ensuring your plans address both passive and active countermeasures is a critical concept in reducing the number of injuries and causalities associated with such a traumatic event. Before we explore passive and active countermeasures, let us address the criticality of communication. After all, how can your employees take action if you don’t have procedures in place to “get the word out”? There are a number of web-based software applications that work really well in implementing emergency mass communications to your employees in a very short period of time (i.e., One Call Now System, AtHoc alerting system, NOTIFIER emergency communications systems, etc.). Whether you utilize one of these applications to quickly e-mail, text, phone call, or simply use intercoms, digital sign boards, bull horns or runners, you MUST have a way to quickly communicate the nature of the ASE, location of the threat and an evacuation route. Most hospitals have a code designated for an active shooter. Usually, the use of a Code Silver notification is synonymous with an event involving a weapon or firearm.

TAKING PASSIVE COUNTERMEASURES

Co-author William Losefsky recently completed the ALICE Active Shooter Instructor course and now has an increased appreciation of training needed to properly prepare employees in implementing countermeasures against the threat, especially when there is no other option.

Webster defines Countermeasures as: “an action or device designed to negate or offset another.” It is designed to prevent an undesirable outcome in the process. Countermeasures can be both passive and active. When we speak of taking passive measures, we are encouraging you to teach your employees to instinctively
think about proper barricading methods (i.e., protect in place). When faced with an ASE, and there is no time to escape, specific locations should have been pre-identified as a recommended *protect in place room*.

These identified “sanctuaries” are rooms which can be locked from the interior, have little or no glass interior windows and often contain walls that provide more protection than that of sheetrock against potential gunfire. Employees should be taught how to quickly barricade the door (i.e., heavy copy machine, desk, hospital bed, etc.) that will add additional “fortification” or help delay an intruder’s ability to enter the room. Emergency Planners should consider placing a silver sticker on the door of any pre-identified “Code Silver Compliant” rooms to aid in employee reaction and protecting in place actions. These markings are especially useful in a hospital environment where employees often move about and may be unfamiliar which room might provide them the most protection.

Other passive measures to consider if forced to protect in place in a room that cannot be locked from the interior: use belts, purse straps or possibly electrical cords to tie a door shut. Additional consideration should be made in purchasing 500 feet of parachute cord which can be cut and distributed into 25 foot sections to those room/offices that cannot be locked. When protecting in place during an ASE, employees must be trained to turn their cellphones off or to “silent mode,” turn out the lights, and move away from doors or windows and to remain quiet!

**DEVICES THAT CAN BECOME WEAPONS IN TAKING ACTIVE COUNTERMEASURES**

In the hospital environment, we are required to place fire extinguishers throughout the facility. These devices can become a formable weapon when considering taking active measures against a shooter. A class B 10-20 pound fire extinguisher planted upside a shooter’s head may incapacitate the shooter and provide the opportunity to overpower him. Additionally, discharging the extinguisher at the shooter may provide sufficient diversion or incapacitation to allow for over-
powering the shooter.

In our ALICE training we learned that throwing an object at a shooter's face is very distracting and may temporarily interrupt the shooter from firing his weapon. In those few seconds, a swarm technique should be initiated. A swarm technique can be a very effective tactic if the shooter enters a room where there are several employees protecting in place. Each employee can grab a limb and affect a “takedown” of the shooter. Swarming the assailant gives the victims strength in numbers. We practiced swarm techniques in our ALICE training and each-and-every time we were able to overpower and overcome the shooter. Notwithstanding, we understand that a real event is much more stressful than the training environment, but the point is: to do nothing is not a plan and does nothing to thwart the attack and lessen the likelihood of injury or death.

Employees must be trained to be familiar with their work areas and that typical office furnishings can be utilized as “Improvised Weapons (IW’s).” A typical desk contains a variety of IW’s: stapler, coffee mug, calculator (yes, even numbers can hurt), rolodex, phone, printer, books, picture frames, etc. A snow globe thrown at even a Little Leaguer’s speed would be an incapacitation tool if it struck a shooter in the forehead! We have even heard of administrative assistants maintaining a can of wasp spray in their desk as a “last line of defense” against an aggressor. These cans are generally large (high capacity) and the spray stream generally extends out 12 – 15 feet!

**ACTIONS TO TAKE TO SURVIVE WHEN A SHOOTER ENTERS YOUR ROOM**

Taking the typical “run and hide” concept to the next level, employees should be instructed on how to discuss what actions they must take in order to survive if the shooter enters their room. It should become instinctive for them to shut the lights off, lock the door (if possible), place barricades at the door, and develop plans on how to “fight” if given no other option. Designating specific locations for employees to crouch, stand and maneuver, helps prepare the team to take immediate action if the shooter en-
ters (i.e., swarm technique). If the shooter gains entry to the room, the shooter will immediately encounter a low light situation, tripping hazards and a team who is prepared to take immediate action rather than becoming easy targets of opportunity for the shooter.

From watching dozens of actual active shooter drills as well as footage from actual engagements and having observed that the eyes of the shooter are focused looking for potential victims, we have yet to see an active shooter concentrate on looking at the floor for potential tripping hazards. Emergency Planners should capitalize on this by training their staffs on introducing IW’s such as tripping hazards as part of their room defense strategy. Tying some belts across a door threshold or tying a several belts between two chairs may be the tripping hazard that tips the scales into an opportunity to implement the swarm technique.

CONCLUSION

We hope that this article will spark some ingenuity and the instinct to “fight to survive” rather than simply sheltering and hoping for the best. We encourage you to take your training to the next level and ensure that the employees in your facility are provided training on how to take passive and active measures that may mean the difference between life or death. If we as security professionals can achieve this, we have accomplished the most important mission for which we have been assigned: protecting our charges!

References

How to avoid having to “run – hide – fight”
James R. Sawyer, CHPA, CPP

Adopting and teaching a “Zero Incidents” philosophy as a partner to “Run-Hide-Fight” education can prevent most workplace violence incidents, the author believes. In this article, he outlines 14 key points for implementing such a prevention program.

By now virtually every Security Director has had the opportunity to watch the short informative video “Run – Hide – Fight”. In fact, many of us have had the opportunity to watch this instructional video time and again. Undoubtedly, the “Run – Hide – Fight” video is an invaluable tool. It’s impossible to quantify how many health care staff have been terrified and bothered by the Vin Diesel replica clad in black opening up with gun fire in a large lobby area. The message here is clear and precise--active shooter situations may occur anywhere and at anytime. And in a nation with more than 320 million guns accompanied by surging sales it is sheer folly to minimize the risk. To quote a retired Seattle Police Chief after a particularly active August weekend in which multiple people were shot, “we are awash in an ocean of guns.” Obviously, Code Silver planning and active shooter response has to...
be a key educational component of every health care security planner.

**ADD A ‘ZERO INCIDENTS’ PREVENTION-BASED PHILOSOPHY**

However, I recommend in the strongest possible way that security planners add a crucial component or companion piece to their “run – hide – fight” educational effort. The companion piece or bookend for “active shooter” is preventing violence by developing a “zero incidents” prevention-based philosophy.

Everyone has heard and in many ways embraced the “zero tolerance” mantra. “Zero tolerance,” I believe, is ill-advised on so many practical levels. We in healthcare tolerate a great deal and we should. Those we serve and support harbor incredible life stressors, such as:

- Medical illness
- Debt
- PTSD
- Joblessness
- Mental illness
- Unemployment
- Medical bills

This list goes on and illustrates why we need to tolerate frustration and anger and such. Also, “zero tolerance” implies by definition that we are responding to a situation after it has occurred at which time we’ll respond with draconian “zero tolerance” measures as part of the event clean up. There’s a stronger, more practical option. Adopt a “zero incidents” philosophy and make it the Siamese twin to your active shooter-Code Silver policy. Do not teach the one without teaching the other.

**THE KEY ELEMENTS OF A ‘ZERO INCIDENTS’ PHILOSOPHY**

We’ll need to teach staff the key elements of our “zero incidents” philosophy. What are these key elements? Outlined are some of the key points that need to be part of your “Zero incidents” strategy and presentation.

1. **Violence is preventable.**

   Drive home this point. Most workplace violence is preventable and this is not something we are taught. The nightly news showcases endless tragedy working off their tried and true philosophy “if it bleeds it leads.” Workplace violence is preventable.
2. In virtually ever case of workplace violence there are warning signs. Teach this to all staff. Your role and goal here is to sensitize all staff to the warning signs of violence. Those warning signs will be verbal, non-verbal and paraverbal. And the signs may and usually will involve all three. Emphasize the warning signs of violence.

3. Teach staff to listen to their intuition. This is huge! Reference Gavin De Becker’s classic book “The Gift of Fear”. Emphasize and reemphasize the crucial need for all staff to listen to their “gift of fear”. Share this quote with staff, “Human beings are the only animals that will sense danger and continue to walk right into it.” Teach staff to contact security immediately if an individual or situation makes them uncomfortable. Again drive this point home. If something feels wrong, report it.

4. Document! Teach all staff that “the faintest ink is better than the best memory” and to write things down. Staff need to learn the 5 W’s – Who – What – Where – When – Why…and How. Share the security truism “if it ain’t documented, it never happened!” Teach staff the critical importance of writing things down. Staff need to document all:
   - Threats
   - Thefts
   - Assaults
   - Unusual circumstances

   *Without exception!*

5. Report threats! Report and document all threats. On an average day there are about 16,400 threats made to American workers. Less than 20% get reported. Healthcare staff is notorious for not reporting threats. Security professionals must emphasize that threats are illegal and must be reported immediately. Ignoring threats and other warning signs leads to disaster and tragedy. In a land with 320 million plus guns we need to be attuned to threats made by angry clients.

6. Emphasize service – service – service and even better customer service. Teach all staff the 10–4 rule. If a client is within 10 feet of you, smile and acknowledge them. If they are within 4 feet of you, greet them. Emphasize that every visitor, every patient, every family member and every staff is an MVP – VIP who
deserves our optimum level of customer service and support. Teach staff that "you have one chance to make a good first impression." Make every effort to make a strong, positive, first impression. Regarding workplace shooters, the only true way to prevent a workplace shooting is to convince the would-be shooter not to make the attempt. Towards that desired outcome a strong, consistent program in offering maximum customer support to all clients is invaluable. Not only is it the right thing to do, but it prevents violence.

7. Teach staff, all staff these non-verbal warning signs:
   a. Nervousness
   b. Keeping hands in pockets and otherwise concealing hands
   c. Tunnel vision/1,000 yard stare
   d. Finger pointing
   e. Personal space violation
   f. Person refuses any eye contact
   g. Heavy breathing
   h. Favoring one side (strong side)
   i. Blading (turning body to protect weapon)
   j. Blocking egress
   k. Adjusting waist band or clothing.

8. Teach staff these verbal warning signs of violence:
   a. Threat of suicide or self-harm
   b. Threat of violence, directly or implied.
   c. Intimidating others, frequently confrontational
   d. Muttering
   e. Increase in pitch when speaking—indicating throat is fighting
   f. Repetitive word use, parroting and or echoing
   g. A nervous laugh or laughing at inappropriate times. Laughing is a way for a body to shed emotions
   h. Talks of seeing red.
   i. Boasts about prior violence
   j. Talks about hurting animals
   k. Trouble communicating
   l. Chronic blaming—"pathological blamers"—where extreme and unrelenting and irrational blame is directed at a particular caregiver. An individual's low familiarity with an area.
9. Teach staff these other important warning signs:
   a. Minimizing door-to-door distance from vehicle (parking in fire lanes)
   b. Repeated entries/exits to area-scoping-checking an area out
   c. Oversize torso or bulky jacket/vest-odd bulky clothing
   d. Undo attention to carried objects.
   e. Small bulges near waist or hip.
   f. Clothes not appropriate for event/weather. An example is a heavy sweatshirt in high summer heat.

10. Teach your team and all staff to “look for clusters” of behaviors regarding verbal and non-verbal behaviors. For example, if someone showcases or demonstrates four to five behaviors, take a serious look at this individual. Someone exhibiting five to seven of the warning signs is a concern and immediate follow up is recommended.

11. Run background checks on those who concern you! “Information is light” as Tom Stoppard so wisely advised us. Security teams must have the ability to run immediate background checks on individuals of concern. Background checks are an effective and an invaluable tool. If a person of concern has three assault convictions that should trigger a security support, intervention plan for that individual. Best practice—know whom you are dealing with. Towards that end background checks are illuminating.

12. If you are a no weapons facility, post No Weapons signs in your facility. Make sure these signs are posted in your parking lots, at entrances and in lobby areas. Best practice—Make sure your “No Weapons” policy is widely shared and understood. Don’t make it an organization’s best kept secret.

13. Have a strong, proactive and vigilant domestic violence support plan for staff. Our national domestic violence statistics are a horror story. One in four women are in a dangerous relationship; add this to a hospital's unique gender ratio—89% female to 11% male and you have the potential for serious events. Build a
strong domestic violence support team that can convene within 8 hours to address, review and build a plan of support for a domestic violence victim. Many workplace professionals limit themselves to what they can do here. However there’s a lot we can do such as:

- Changing locks
- Providing transportation
- Providing taxi vouchers
- Providing safe housing—hotel
- Modifying schedules
- Changing parking assignments
- Contacting and trespassing perpetrators

That just lists a few. The key is to take this matter seriously and respond immediately. This is not “just a Human Resources matter.” Addressing domestic violence is a sentinel security challenge and an enduring priority.

14. Contact perpetrators!
This is key. A key integral component of “zero incidents” planning is contacting people, individuals of concern. You must have this ability. Contact may include:
- A certified letter
- A regular letter
- A courier message—process server
- Email
- Phone call
- All of the above

Proactive security planners must have the ability to contact directly individuals of concern. This is invaluable on so many levels. One, it lets the individual know you are aware of them which is huge. Two, it gives you and your team the ability to actually talk and interact with an individual of concern. That by itself is invaluable and if the appropriate respect and customer service skills are utilized in the initial contact then a potentially violent situation may be prevented. This is the heart of “zero incidents” planning.

SUMMARY

“Zero incidents” is the goal every security planner should work to achieve. The tools to build a “zero incidents” environment involve:

- Acknowledging that violence is preventable.
- Providing optimum customer service to every visitor, patient, family member. They are all
VIP’S.

- A strong emphasis on documentation.
- Honoring and responding to staff intuition.
- A proactive threat response program-policy.
- Teaching all staff the verbal/non-verbal warning signs of violence.
- Proactively contacting individuals of concern, making direct contact.
- Having a strong domestic violence response and support plan.

Active Shooter and Code Silver planning should also involve the crucial component of violence prevention and “zero incidents” philosophy. By merging these two, security planners will achieve the best of all possible outcomes. They will teach staff how to run, hide and fight and at the same time build a culture and workforce that provides both maximum customer support and staff awareness.

### Frequently Asked Questions

| Q: How valuable are “Active Shooter” classes? | A: Of huge value especially if violence prevention and “zero incidents” philosophy are woven into it. |
| Q: Is “Zero Tolerance” not desirable for hospitals? | A: It’s simply not accurate as we tolerate a lot and should. Of course, once an event occurs having universal and identified response standards is wise. However, it’s much preferred never having to respond. |
| Q: How important are background checks? | A: For security it is huge. Knowing whom you are dealing with is always a best practice. |
| Q: Regarding “zero incidents” philosophy, are there any other best practices for staff? | A: Yes one universal: never, ever under any conditions meet an angry individual one on one in an isolated area, never. |
| Q: If gun violence comes to a hospital, what are two areas where such violence could manifest? | A: Focus on domestic violence, you can’t ignore that, and watch for “blamers,” |
Frequently Asked Questions (continued)

"pathological blamers" or "collectors of injustice". Key--sensitize yourself to those who place extraordinary or unusual blame on a particular caregiver.

Q: What's the trend regarding "active shooter" in hospitals?
A: There appears to be "more active shooter" incidents but in many cases violent crime is down. However the sheer numbers of weapons and the ease of accessing guns compel us to prioritize this training.

Q: How much priority should we give to suicidal patients, family members?
A: Lots and lots of priority. Security planners need to respond to any and all reports of self-injurious commentary. Suicides in hospitals' unfortunately are a problem and a challenge that may grow in scope.

Q: Do you recommend that security teams conduct annual safe gun handling classes?
A: Yes, absolutely.

Q: Should security maintain weapons storage safes?
A: Yes. Look into it. Security should maintain a safe secured area to store firearms.

Q: Regarding No Weapons signs. Is placement everything?
A: Yes. Location is everything. Focus on parking lots and main entrances.

Q: Is it hyperbole or is it accurate and true that the best most viable, violence prevention strategy devised is an aware workforce committed to optimum customer service?

Q: So we should promote to all staff the concept of "making a good first impression."
A: Shout this from the highest hills.

Q: Should all new employees have violence prevention training from the outset?
A: Yes, absolutely. This has to happen.

Q: Regarding domestic violence, how important is it to address family, violence situations quickly?
A: This is of priority importance. You cannot emphasize this enough.

Q: Should security contact and trespass domestic abusers?
A: Yes

Q: Should you have the victim's approval here?
A: Yes, without exception. The victim must approve any and all actions that you take on their behalf.

Q: When should we start teaching all staff about the importance of honoring their intuition?
A: This should be heavily emphasized from Day One.
According to the author, researchers have found that violence experienced by healthcare staff is associated with lower patient ratings of the quality of care.\(^1\) Now that hospital reimbursements are more severely related to patient experience, she adds, health care employers' bottom lines will also feel the effects of workplace violence.\(^2\) Hospitals and healthcare leaders have always been concerned with violence for obvious reasons. Now they have a new reason—and it's directly related to reimbursement. Patient experience and violence can negatively impact the bottom line for hospitals, and that is driving a renewed interest in developing highly qualified Threat Assessment Teams (TAT) which can make a difference. In this article, she provides guidance on how to form effective teams.

(Lisa Pryse Terry, CHPA, CPP, is Director of Hospital Police and Transportation at UNC Health Care, Chapel Hill, NC. She formerly served as Division President and Chief of Company Police of ODS Healthcare Solutions, Raleigh, NC, Campus Police Chief of Eastern Virginia Medical Center, Norfolk VA, and Director of Public Safety of WakeMed Health and Hospitals, Raleigh, NC. A past-president of the IAHSS Board of Directors and current member of the Healthcare Council of ASIS, she currently serves as an advisor to ODS Security Solutions and is a board member of the North Carolina Company Police Chief's Association.)

**PURPOSE OF THREAT ASSESSMENT TEAMS**

The consequences of workplace violence have real ramifications for healthcare delivery.

Hospitals and healthcare leaders have always been concerned with violence for obvious reasons. Now they have a new reason—and it's directly related to reimbursement. Patient experience and violence can negatively impact the bottom line for hospitals, and that is driving a renewed interest in developing highly qualified Threat Assessment Teams (TAT) that can make a difference.

Assessment of Healthcare Providers & Systems (HCAHPS) is among the measures to be used when calculating value-based incentive payments in the Hospital Value-Based Purchasing Program. HCAHPS measures patient experience and satisfaction rates. Reimbursement rates and financial incentives for healthcare facilities are based on many other factors under the ACA, including readmission rates. TATs have an
opportunity to positively influence factors that affect reimbursement. By identifying potential risks of violence and threats, they can create an ED environment more conducive to treatment, healing, and a positive patient experience.

Joint Commission standards also specifically address the requirement for hospitals to conduct threat/vulnerability assessments and ensure the safety of everyone within the facilities. TJC standard EM01.01.01 includes instructions that the hospital must conduct a hazard vulnerability analysis to identify potential emergencies that could affect demands on the facilities. They must determine if the hospital facilities have the resources to provide services and patient care in the event of a disaster or sentinel event and the consequences of the events. All findings and recommendations must be clearly documented. TATs play a key role in addressing this TJC standard along with many others (see box on this page for examples of TJC requirements impacted by TATs.)

Experienced TATs are key to conducting comprehensive threat assessments for healthcare facilities. They are integral to development of the threat management and violence prevention programs. They also support development of threat management

| Examples of TJC requirements with an impact on physical environment: |
| Life Safety (LS) |
| Environment of Care (EC) |

includes functional areas:
- Safety
- Security
- Smoking
- Hazardous materials/waste
- Fire safety
- Medical equipment
- Utility systems (emergency power, other)
- Provision of a safe, functional environment
- Emergency management (EC) Planning
- Emergency operations plan
- Managing operations through an emergency
- Evaluating effectiveness

Note: This is not an exhaustive and prescriptive list, but it serves as an example of how the TAT and annual Threat Assessment can positively impact the hospital.
strategies and processes that mitigate risks and eliminate threats of violence wherever possible.

The team is responsible to:
- Ensure 24/7 security
- Conduct comprehensive assessments and investigations
- Plan and implement risk reduction strategies
- Determine appropriate interventions
- Oversee remediation and work plan management
- Document findings, recommendations, and strategies
- Contribute to the overall safety of the organization. The TAT conducts their evaluation by taking a detailed look at the workplace to identify existing and potential hazards for workplace violence. The team analyzes and tracks, records, monitors trends, analyzes incidents, delivers screening surveys, and examines overall workplace security. They also evaluate engineering controls, administrative and work process controls, and post incident response.3

BUILDING YOUR TEAM

Members of the TAT have varied responsibilities throughout the organization. They bring a multitude of perspectives from their respective areas of responsibility, creating a comprehensive overview of the entire facility. In an interview with Gene Deisinger, Ph.D., Deputy Chief and Director of Threat Management at Virginia Tech Police Department, Deisinger discussed the threat management team concept.

Dr. Deisinger is also a founding member of the Iowa State Critical Incident Response Team (CIRT), and he explains:

In the early 1990's we experienced a set of crisis situations that illustrated the need for greater communication, collaboration, and coordination among university departments. We identified situations where individual departments had (or were aware of) information that turned out to be relevant. However, key decision makers in other departments, impacted upon by the person or situation, were not aware of that information. Therefore, they held an incomplete picture of the situation as it actually existed. We also observed that individual depart-
ments brought to bear a wide range of expertise and resources, but typically implemented their approaches to crisis situations independent of other involved departments. On occasion, this resulted in escalation of the crisis that was not anticipated (because no one was looking for it), and for which we were not adequately prepared to manage.4

According to Dr. Deisinger, the TAT should include individuals based on the needs of the organization, the likely threats, and the available resources. He cautions on the importance of not holding one position or individual responsible for assessing and managing threats, but instead to establish a comprehensive team. Assessments should be conducted and evaluated through consultation and collaboration with other individuals trained in assessment and management of volatile situations.5

While security professionals have the experience and training to identify and deal with threats, clinical departments, human resources, administration, and other areas should also be engaged. They contribute important information regarding hospital policies, procedures, legal implications, regulatory requirements, and other critical information. Even though the highest rates of violence occur in the ED, there are many other considerations to evaluate when developing threat assessment policies and procedures. These ancillary department representatives are vital to the TAT and will ensure compliance with HR requirements, legal considerations, and other areas of management.

Behavioral health specialists and psychologists are examples of valuable team resources too. These professionals offer insights into the potential behaviors and actions of people who are emotionally disturbed, angry, upset, or depressed. They are also able to better identify methods to reduce risk and serve as resources for remediation to support systems that help de-escalate events.

Ensuring all areas of the hospital are included on the TAT is one way to improve communication and gain a more complete picture of potential threats. Individuals from various areas of the organization bring a wide range of expertise and resources to the assessment process—identifying
threats that might have been otherwise overlooked. Multidisciplinary teams are much more effective than a team comprised only of representatives from a single department.

Considerations for the team include, but are not limited to:
- Hospital administrators and leaders
- Security staff members/leaders
- Nursing administration
- ED and behavioral health staff
- Local law enforcement
- Risk management
- Human resources
- Legal counsel
- Employee assistance
- Mental health and counseling services
- Union representatives, if applicable
- Ad hoc members as deemed appropriate.

The goal is to include team members who bring varying levels of expertise and experience to the group. Healthcare threats often come from the most unsuspecting sources, so a team of individuals with breadth and depth of experience is essential. The team investigates actual threats, but conceptual threats are also their responsibility. Foreseeable events derived from conceptual threats are more obscure and typically do not occur on a frequent level—leaving them often uncovered until an actual event occurs. An experienced TAT is more likely to identify actual and conceptual threats. Healthcare threats are dynamic, changing from day to day. That requires a vigilant TAT that is able to fully engage in investigative processes, analysis, and remediation. It is a dynamic process that must be repeated and updated periodically. The TAT must have the aptitude and experience to identify real or perceived threats. The TAT is also responsible for supporting organizational training relative to security and safety. According to OSHA recommendations, the team provides training to help employees identify and manage workplace violence and other threats. They must ensure that all employees understand the concept of universal precautions for violence and personal safety that refers to the concept that violence must be expected but can be mitigated or managed through precautions.6
The Threat Management Team Concept

- **Ongoing Program Evaluation**
- **Strong Management Commitment**
- **Continual Training**
- **Employee Involvement**
- **Hazard Reduction and Response**
- **Ongoing Worksite Analysis**
THREAT ASSESSMENT
TEAM MEMBERS

An evolving best practice is to have two separate teams to help manage and oversee potential threats of violence. The University of North Carolina (UNC) Healthcare System recently implemented a Disruptive Patient Assessment Team (DPAT) to conduct assessments every 12 and/or 24 hours for behavioral health, forensics, and other patients who pose a threat to themselves or others. This DPAT is in addition to the general facility-wide TAT responsible for overall security assessment and management. Both teams serve a critical role by enhancing the level of security and safety for patients, staff, and others. Although there should be other healthcare professionals on the TAT as previously discussed, it’s essential to have highly trained and qualified security professionals leading the general TAT. These individuals have very specific healthcare security training, background, and experience that includes clarity on regulatory agencies and specific requirements. On the other hand, smaller clinical teams such as the DPAT may be led by a clinical staff member and supported by members of the security department. The same logic applies to the value of bringing varied disciplines to the group for assessment and evaluation of potential threats of violence. When considering who should be on the team and who should lead each team, there are helpful guidelines. OSHA guidelines cite the significance of having individuals with the appropriate level of expertise and training in workplace violence prevention in healthcare and/or social services:

Assign responsibility and authority for the program to individuals or teams with appropriate training and skills. Ensure that adequate resources are available for this effort and that the team or responsible individuals develop expertise on workplace violence prevention in health care and social services.

Team members for TATs and DPATs must be sensitive to individual legal and civil rights, confidentiality regulations, cultural concerns, and other factors driving actions. They must respect the differences in individuals while protecting everyone equally. Security and protection extends to
clinical and ancillary staff, patients, family members, and visitors. High-risk patients such as forensic patients and behavioral health patients must also be considered and protected.

**GENERAL THREAT ASSESSMENT TEAMS**

The core team leaders include:

- **The Director of Security.** This leader should be educated and well credentialed in the very specific field of healthcare security with training such as IAHSS, ASIS, and others. The person must clearly understand direction by regulatory organizations and related requirements. This person should also have strong general leadership skills, including strong communication and problem-solving skills.

- **Security officers.** Experienced officers should be trained in healthcare-specific security issues as well. AMA, elopement, EMTALA, HIPAA, CMS, and restraint and seclusion are just a few examples. Officers should be fully trained in nonviolent crisis intervention techniques, state laws with oversight for security officers, personal defense tactics, IAHSS Security Officer training, and/or similar backgrounds and training.

A diverse team of individuals can enhance security and contribute to the TAT when led by a qualified security leader. Team members bring varying strengths and insights to the overall group, strengthening the safety and security of the organization.

**DISRUPTIVE PATIENT ASSESSMENT TEAMS**

Smaller teams focused on a daily assessment of patients at high risk for violence may be responsible for responding to the increased number of healthcare assaults. A clinician with strong leadership skills and experience in de-escalation and management of violent individuals often leads this team. Individuals from various departments support the team leader, including security, human resources, social services, or other relative specialties.

The DPAT is clinically driven, and the interval of assessment required is based on clinical discretion in most cases. Diagnosis, behavior patterns, medication issues, recognized threats, and other factors may deem it appropriate to conduct 12-hour or 24-
hour patient assessments to mitigate risk. It is important to ensure the assessment process does not give the patient a feeling of being policed or watched. The DPAT assessment team member can demonstrate concern for the patient and address him or her with compassion and caring, which alleviates concerns and contributes to a positive patient experience.

The UNC Health Care System (NCHCS) is an example of an innovative leader in establishing this type of assessment team. The objective of the DPAT is to address disruptive behavior and to ensure optimal patient care and continuous healthcare service delivery. Team members of the NCHCS DPAT may be appointed by:
- The Chief Nursing Officer
- Associate Vice President of Risk Management
- Accreditation and Regulatory Affairs
- Others as appropriate

The team may consist of:
- House Supervisor from Adult Medical/Surgical Services
- Psychiatry clinicians
- Nursing Director
- UNC Hospitals Police
- Patient Relations
- Legal and Risk Management
- Patient Registration
- Other UNCHCS departments as deemed appropriate

This is a very specialized multidisciplinary team responsible for assisting hospital units or providers in developing plans and strategies to manage disruptive patients or visitors. They determine when patients should be added to an “Alert List,” notify patients and/or visitors of limitations on any access to UNCHCS facilities, collect and analyze incidents and data on disruptive individuals, and identify training needs related to prevention and management of disruptive behavior.

The team creates and maintains an alert system to identify individuals who have engaged in disruptive behavior on the property and develops appropriate guidelines for managing those individuals. This is a very proactive approach to mitigate violence that is not only effective, but contributes to the overall patient experience for the facility. The DPAT model serves as a best practice for other hospital EDs.
HOW THE THREAT ASSESSMENT TEAM SUCCEEDS

According to NIOSH, "To prevent violence in hospitals, employers should develop a safety and health program that includes management commitment, employee participation, hazard identification, safety and health training, and hazard prevention, control, and reporting. Employers should evaluate this program periodically. Although risk factors for violence are specific for each hospital and its work scenarios, employers can follow general prevention strategies."

The first thing to remember is that establishing TATs is a best practice as much as a legal requirement. Establishing an effective TAT and DPAT is the right thing to do in healthcare where patients, staff, families, and visitors expect safety and security. If you’re doing it for any other reason, success is less likely to occur.

The role of team members is to assess and manage threats and threatening behavior, anticipating events before they occur when feasible. They succeed by carrying out their primary mission to assess the likelihood of violent events and, secondarily, to determine the best methods of intervention. Patient and staff safety are always key factors in their considerations and recommendations.

As stated above by NIOSH, violence prevention requires hospitals to develop programs based on management commitment. The TAT and DPAT succeed with the support of hospital administration and management. It’s critical to have the C-suite, hospital leadership, security management, and other parties fully engaged in the process. Assigning responsibility and ensuring individual team members accept accountability leads to the highest levels of success. Threat assessment is a continuous process, and the teams require continuous support.

The key drivers of success for the TAT and DPAT create a dynamic process for vigilance and constant evaluation of effectiveness. The most effective TAT members are constantly aware of their environment and routinely assess situations for signs of any threats.

To succeed, the team members must identify and assess threats. They must have the skills, experi-
ence, and ability to:
- Identify potential perpetrators and areas of high risk
- Assess risks of violence
- Manage the individual and risks to others
- Recover from an event

While some team members may be highly experienced, others are new to the process. It’s important to orient them to the team and provide necessary training and overview of expectations. Their orientation may include training on how to effectively evaluate risks by providing specific examples. The important thing is to allow team members to use their creative thought processes to evaluate and analyze situations.

RISKS TO THE TEAM

When the team members work together collaboratively and understand individual roles and responsibilities, they are powerful if violence erupts. But, both the TAT and DPAT run the risk of being ineffective if not supported and managed properly.

Authority. Dr. Deisinger points out that a common mistake and risk of a TAT of any type is the lack of clear authority to fully manage threatening situations and manage critical situations. Since threats of violence occur quickly and often with little warning, decisions must be made quickly before situations escalate. Having a clear line of authority and recognizing the primary decision-maker is essential. This allows the responsible individual to assess the information, consider a reasonable range of interventions, and then direct implementation of a specified strategy.

Complacency. Another major risk of threat to the TAT is complacency. Threat assessment is not a temporary assignment or event. It is a dynamic process conducted by a team of individuals who are continuously engaged in assessing potential threats and mitigating risks. In times of low threats, the TAT may fail to remain active and continually review their policies, procedures, communications, and other aspects of threat management. Teams should always be led and directed by experienced training security assessment and/or clinical professionals who work collaboratively with all team members and keep them engaged. A strong leader will recognize the risk of complacency to the team and manage
them well.

**Ongoing management.** Lack of ongoing management support puts the effectiveness of the teams at risk. Without the continuous backing of the C-suite and other leadership team members, the effectiveness of the team is diminished. The TAT or DPAT leader should be fully engaged and should motivate the team for continuous success.

**Resources.** Finally, a lack of resources puts the team at risk. Success is contingent on providing team members with the data collection tools and resources necessary to assess threats. Routine meetings and periodic updates keep members engaged and focused on their mission. Provide team members with specific deliverables and timetables for completion where applicable, and recognize them for a job well done to avoid complacency. Give them the tools and resources to succeed, and encourage continual improvements and enhancements.

The ultimate goal is to establish an effective team to minimize the opportunities for violence and alleviate risks through preparation and prevention. And if violence does occur, as it eventually will, to respond swiftly and appropriately. Charge the team with carrying out their duties and responding to the direction of NIOSH:

*Violence may occur in the workplace in spite of preventive measures. Employers should be prepared to deal with the consequences of this violence by providing an environment that promotes open communication and by developing written procedures for reporting and responding to violence. Employers should offer and encourage counseling whenever a worker is threatened or assaulted.*

Once the TAT has been established, the real work begins. Conducting routine and thorough threat assessments becomes their number one priority. TATs are the backbone of an effective workplace violence and threat management program.

**References**


2. Ibid.


7. Source: Lisa Terry, CHPA, CPP. Director of Hospital Police and Transportation at UNC Hospitals; Advisor to ODS Security Solutions.


(This article is excerpted with permission from the author’s book, Preventing Emergency Department Violence. Tips and Tools to Keep Your Facility Safe, published by HCPro. E-mail: customerservice@hcpro.com or online at www.hcpro.com. For further details and contents, or to order, go to http://hc-marketplace.com/preventing-emergency-department-violence-tips-tools-and-advice-to-keep-your-facility-safe)
Emergency codes: a study of hospital attitudes and practices
Alexandra Mapp MPH, Jennifer Goldsack, MBA, MChem, MA, MS, Leslie Carandang, James W. Buehler MD, and Seema S. Sonnad PhD

Emergency color code designations which differ from hospital to hospital have been identified as potential causes of confusion which can exacerbate the problems caused by the emergency itself. This study seeks to measure preferences for standardization of emergency codes on the part of hospital administration, hospital staff and patients.

Abstract
Many hospitals use color codes to denote internal (i.e. patient respiratory distress), or external (i.e. natural disasters) emergencies, via public announcement systems. Variations in the codes used by different hospitals can create confusion among providers who may practice in more than one hospital. This study sought to understand emergency code practices in the Delaware Valley region, assess patient and provider knowledge of codes at one hospital in that region, and patient and provider preferences for emergency code standardization and format. Anonymous electronic surveys on procedural knowledge and perspectives of emergency codes were disseminated to hospital staff and patients located at a large regional hospital. Phone interviews were conducted with hospital administration at the regional hospital and other hospitals within a 50-mile radius. The au-
thor’s research indicates that standardization would be accepted by patients and providers and its lack is considered a barrier to providing high quality care.

INTRODUCTION

Hospital emergency color codes allow rapid staff response to emergency situations within hospitals. These color codes are a part of every hospital’s emergency response plan. The Joint Commission, an organization that certifies and accredits hospital care organizations and programs in the United States, mandates that every hospital must have an emergency management plan. However, their mandate does not indicate the extent to which plans must follow a specific format, nor do they indicate a system for assigning different internal and external emergency situations a distinct color code. Under the current system, hospitals are tasked with creating their own system of color codes. As a result, these emergency codes do not follow an identifiable standard. Lack of uniformity is problematic not only in efficient emergency management but also in the context of patient safety. Individual hospital associations are attempting to reduce variation by recommending a standardized set of color codes, although standardization is not mandatory.

The Hospital Association of Southern California’s standardized set of emergency color codes includes the most common “Code Blue” and “Code Red” as well as “Code White” to denote a pediatric medical emergency, “Code Gray” to denote a combative person, and “Code Purple” to denote child abduction. In addition, many hospital associations and federal organizations (U.S. Department of Health and Human Services and U.S. Department of Homeland Security) are beginning to embrace changing the formatting of codes using a plain language approach. Hospital associations that support plain language do so as a means to increase hospital transparency and hope it also will contribute to improved patient decision making. The Institute of Medicine defines health literacy as the level at which health consumers can make a health decision based upon the clarity of information they receive and process and hospital transparency can be contrib-
utory in increasing health literacy.\textsuperscript{5}

Nine state hospital associations, including California, Washington, Florida, Maryland, and Ohio have expressed concern over the lack of standardization and proposed individual sets of standard color codes, available for adoption on a voluntary basis. Only Maryland has mandated standardization.\textsuperscript{6}

Following an active shooter incident at an Orange County hospital, a statewide standardization initiative in California began in July 2007. Results from a 2011 survey of 240 member hospitals published by the California Hospital Association show that nearly 100 percent of participating hospitals use “Code Red” and “Code Blue” to denote a fire emergency and a medical emergency, respectively\textsuperscript{7}. This finding reflects the use of “Code Red” and “Code Blue” across the country. However, uniformity of emergency codes across hospitals was practically non-existent for less commonly used codes (such as code orange or code black). These results led to greater efforts by the American Hospital Association and states to standardize emergency codes nationwide. A parallel proposal to standardizing the use of color codes is moving away from color codes to plain language (e.g. “Medical emergency on the third floor” instead of “Code Blue on the third floor”).

For ease of use and increase to hospital transparency or hospital literacy, states like Minnesota have begun to mandate that their hospitals move toward plain language.\textsuperscript{8} By adopting plain language for emergency communication, states like Minnesota hope to reduce staff confusion for those holding appointments at multiple hospitals, prevent delays of care, and increase patient safety.\textsuperscript{9} Additionally, emergency code uniformity enables hospital staff that work across multiple facilities to respond appropriately to specific emergency situations, allowing for ease in mitigating hazards to their own safety, as well as the safety of patients and visitors.

Non-uniformity in emergency codes poses significant threats to patient safety. Code confusion or responding based on an incorrect understanding of a code, such as calling for law enforcement when the appropriate code should be a medical emergency is known to...
adversely impact outcomes. A recent study identified 154 hospital related shootings from 2000 through 2011, of which 59% (n=91) took place inside the hospital. Slow or inappropriate response to this rare event would likely result in significant morbidity or mortality to patients, visitors and staff.

Given the limited research evaluating emergency hospital codes, the objective of this study is to develop a better understanding of emergency code procedures and provide evidence of patient and provider attitudes about standardization and plain language.

METHODS

This was a survey study conducted in a region where multiple states intersect and it is not unusual for both staff and patients to spend time in hospitals in more than one state.

Population. The study population consisted of three groups: Hospital Administrators, Hospital Staff, and Patients. Hospital administrators were selected from all “acute-care” hospitals within the Delaware Valley Region. Hospital staff and patients were randomly selected from Christiana Care Hospital in Newark, Delaware. Hospital staff included nurses, physicians, technicians, physician’s assistants, per diem, residents, ancillary staff, and temporary staff. Patients were approached for participation while they were waiting in Christiana Care settings with overhead paging including the emergency and trauma services, pediatric ward (parents were interviewed), maternity, cardiology, and cancer center. The final sample included 66 participants: 6 hospital administrators, 47 hospital staff members, and 13 patients.

Data Collection. Data were collected using three separate surveys. Hospital staff and patient surveys were administered in person but responses were anonymous and recorded by the interviewer or responses were anonymously recorded onto a tablet by the participant. For hospital administrators, surveys were conducted over the phone without recording any identifying information.

The surveys covered both current emergency color code procedures and perception and attitudes about plain language. Questions gathered information about the
current emergency code system, efficiency of the current system, opinions standardization, and perceptions of plain language. Hospital Administrators additionally provided information about procedures and training, staff and personnel feedback on color codes, and issues with current code systems as well as their opinion on switching to plain language. Hospital Staff surveys included questions regarding procedures and training on hospital codes, knowledge of the codes used at CCHS, and feedback and perspectives on a plain language approach. Hospital Patients answered questions regarding their familiarity with color codes, perceptions about plain language and their preference for plain language versus color codes.

Analysis. As data were both qualitative and quantitative, we employed a mixed methods analytic approach. The qualitative analysis included thematic coding of feedback from hospital administration, staff, and patient surveys to identify consistent themes in responses. The quantitative component of the study included descriptive statistics, frequencies and percentages of questions with

Likert Scale responses.

RESULTS

Hospital Administration. Hospital Administrators (N=6) indicated that employees received training on hospital emergency response procedures, including hospital color codes, during orientation at the beginning of hire. In addition, hospital administrators identified the following methods of employee training and retraining:

- Annual re-education of employees including modules on emergency codes
- Monthly drills on randomly selected color codes
- Post code activation analyses including competency assessment and feedback on procedure
- Annual safety fair with a mandatory test including questions on codes

Common feedback received from hospital staff by hospital administrators included concerns about a lack of emergency code standardization and consistency with selected colors, at staff members’ respective hospitals and hospitals in general. One
administrator indicated that there was “over instruction” on emergency code procedures and that plain language should be adopted. Other feedback included recommendations to eliminate certain non-clinical color codes such as code grey or code orange (bomb threat and hazardous material spill) and the observation that codes are not activated appropriately in many situations.

Administrators expressed varying opinions on whether a plain language system should be adopted. Those opposed to plain language felt that it could “upset” or “bother” patients and is the “biggest security no-no”. However, those in favor of a plain language approach felt that codes related to persons with weapons and natural disasters would benefit from the switch, including the ability of plain language to improve the appropriateness and speed of patient and visitor responses upon hearing an emergency directive.

**Hospital Staff.** With regard to code procedure, 77% of staff participants were able to recall the procedure for activating emergency color codes. However, 40% indicated that they have witnessed code confusion either during an emergency response drill or during real time. Code confusion can most commonly be attributed to code inconsistency between different regional hospitals and staff rotation and 41% of personnel interviewed had previously worked in hospitals with color codes that differed from Christiana. When hospital staff participants were asked specifically to identify current color codes and their meaning, most were unfamiliar with security codes such as gray and yellow.

Staff feedback and opinion on plain language, as presented in Figure 1 and Table 1, indicate that a shift to plain language is generally supported and those who were agreeable to switch cited clarity and decrease in confusion as the main benefits. For those staff who expressed disagreement with a plain language system, it is interesting to note that their issue with plain language primarily centered on patient risk perception and stress.

From the perspective of plain language and hospital transparency, hospital staff expressed similar sentiments as with the general plain language system
Figure 1. Hospital Staff – Is Plain Language Better than Codes?

Table 1. Hospital Staff Comments on Whether Plain Language is Better than Codes

<table>
<thead>
<tr>
<th>Hospital Staff who “Strongly Agreed” or “Agreed”: Plain language is better</th>
</tr>
</thead>
<tbody>
<tr>
<td>“Much more clear for patients and staff.”</td>
</tr>
<tr>
<td>“Would decrease confusion trying to remember all these codes.”</td>
</tr>
<tr>
<td>“Wouldn’t have to think about it.”</td>
</tr>
<tr>
<td>“Not everybody knows the codes”</td>
</tr>
<tr>
<td>“Everyone understands it.”</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Hospital staff who “Strongly Disagreed” or “Disagreed: Plain language is better</th>
</tr>
</thead>
<tbody>
<tr>
<td>“Because [we] don’t want to upset visitors and patients.”</td>
</tr>
<tr>
<td>“Might cause alarm and other questions from patients...could lead to HIPAA violations.”</td>
</tr>
<tr>
<td>“Visitors may become unduly alarmed if the code system is dropped.”</td>
</tr>
<tr>
<td>“If folks know the shorthand code systems (blue, delta, etc.), you immediately know the nature of the code. Plain language would need to be more wordy.”</td>
</tr>
<tr>
<td>“On some instances announcing plain language may cause panic among patients and visitors.”</td>
</tr>
</tbody>
</table>
Although a relatively small percentage of staff disagreed with the notion that plain language would increase transparency, their feedback (Table 2.) was plentiful and highlighted a common theme that codes should be meant for staff only as decreasing patient stress within a hospital setting is just as important.

**Hospital Patients.** Ten of the thirteen patient participants were familiar with Code Red and Code Blue. Code Blue (the medical emergency code) was most frequently cited as the code that should not be changed either in color or to plain language. As presented in table 3, patient feedback on plain language underscored the common theme of transparency within the hospital setting and providing the most thorough information, especially during situations requiring emergency response.

Table 4 illustrates some of the feedback from patients regarding whether they have a preference for either system of emergency response (codes versus plain language) and which would provide for increased patient safety. Patients were split equally between preference for plain language and for codes and their perceptions concerning feelings of safety elicited by either system. Those patients who preferred the plain language and felt it safer echoed the need to know what is going on in the environment around them. For those patients who demonstrated preference for the current coded system and felt it safer, trusted that the coded system, which has already been in place, is best as it is most widely known.

**DISCUSSION**

Results indicate that administrators, staff and patients all view code standardization as having potential to improve both patient safety and disaster preparedness and response. It was interesting that all study groups felt that while a plain language approach would increase hospital transparency that may not actually be desirable as the use of colors shields patients from unnecessary or undesirable information.

Although transparency is a part of the plain language approach, our evidence suggests that transparency for the sake of health literacy is not the general concern of the hospital patient. Patients are aware that emergency response
Figure 2. Hospital Staff – Would Plain Language Increase Hospital Transparency?

<table>
<thead>
<tr>
<th></th>
<th>Strongly Agree</th>
<th>Agree</th>
<th>Neither Agree nor Disagree</th>
<th>Disagree</th>
<th>Strongly Disagree</th>
</tr>
</thead>
<tbody>
<tr>
<td>%</td>
<td>15</td>
<td>52</td>
<td>15</td>
<td>7</td>
<td>9</td>
</tr>
</tbody>
</table>

Table 2. Hospital Staff Comments on Whether Plain Language Would be beneficial in Increasing Transparency

<table>
<thead>
<tr>
<th>Hospital staff who “Strongly Disagreed” or “Disagreed”</th>
</tr>
</thead>
<tbody>
<tr>
<td>“Don’t think that people, regular public, should know everything that’s going on...could misinterpret.”</td>
</tr>
<tr>
<td>“Should determine/define what is appropriate regarding transparency. Not sure I agree that specifics for codes are appropriate to disclose as it is an organizational response.”</td>
</tr>
<tr>
<td>“Transparency is good but information in the hospital setting needs to be directed to staff who understand response protocols. The risk to visitors is that they become unduly alarmed or confused.”</td>
</tr>
<tr>
<td>“Don’t see transparency as a goal. Goal is to respond appropriately to the urgent/emergent situation.”</td>
</tr>
<tr>
<td>“I am not convinced that this type of transparency is good.”</td>
</tr>
</tbody>
</table>
protocol within a hospital is tailored specifically for those who are tasked as first responders in such situations. Taking into consideration that health literacy serves a more generalized population and not strictly the healthcare professional or staff, the patient perspective aspect of plain language should shift from a complete transformation to a potential hybridized system that involves a mixture of both. Standardization, however, is supported not only by study participants but also by hospital associations, disaster preparedness groups, and state health services. Perhaps the dialogue surrounding changing the system altogether should be focused instead on mandating a standardized system of color codes, as this method is the most familiar.

Emergency color codes exist as a “coded” system to protect patients and were never meant to exist outside of the internal functions of a hospital’s emergency response plans. Maintaining a level of patient and hospital staff safety in an era where there have been increased incidents of mass casualty events, increased safety is as important as ever. Standardization is the best approach to reach a level of consistency in responding to incidents that not only involve patient health but patient and hospital safety as well. Once standardization is achieved, the conversation should then shift towards incorporating plain language versions of emergency situations that involve an active shooter, facility evacuation, or any type of situation where there is a high potential for patient and staff casualties. These codes, although not used often, are the type of codes where expedient response is of the utmost priority as its lack could have fatal consequences.

While it is a progressive step towards standardizing emergency color codes, state hospital associations that already have an existing standardized list of codes should consider collaborating between the states that have similar emergency code policies to create one standardized list completely. A collaborative effort in constructing a standardized system will perhaps provide a starting point for other state hospital associations to do the same. In addition, most hospitals would benefit from yearly retraining of employ-
Table 3. Patient Comments on Perception of Selected Emergency Codes vs Plain Language

Announcement of “Medical Emergency” versus “Code Blue”

“I think that [medical emergency announced instead of code blue] would be a good idea because you know what’s going on, I think it’s good to inform people.”

“I would feel better. Words [like] “code blue” from TV like the doctor shows, means something serious. Medical emergency doesn’t make you think of the “worst”. Code blue would make you panic…like your last straw whereas medical emergency could be many different things.”

“I’d be more amenable to plain language…would be nice because I’d feel like I know more what’s going on. There’s already so much that you don’t know.”

Announcement of “Missing Person” versus “Code Yellow”

“I would prefer ‘code yellow’. Gives you more sensitive [sic] to the situation.”

 “[I am] here under a stressful condition, why would you want to know more that you need to know.”

“Would prefer ‘code yellow’… don’t know code missing person is scarier.”

“I would feel safe”

“Might alert the people in the hospital, in this situation, plain language might be better… depends on the situation.”

Table 4. Patient Comments on a color codes system versus plain language and safety

“Plain language for preference and in the community…workers are supposed to know but the average patient wouldn’t know it and workers would forget the colors [if] they aren’t used often.”

“Codes would be better.”

“Plain language is better because we know what’s going on.”

“Plain system is safer…I want to know what’s going on.”

“No preference…in terms of safety…I don’t think one way or the other…depends on where you are.”

“Codes are in place for a reason, good portion of them are well thought out…”

“Code system might be safer…already know what blue and red mean. In a long stay, only ever heard blue and red.”

“I think I like the codes…would keep from upsetting the patients…you don’t really know exactly what’s happening. Codes would be safer.”

“I would say plain language…there’s so much doctor/nurse language already when they talk to each other, not necessarily talking over me but just talking to each other. With plain language, I’d have more a sense of what’s going on around me. Plain language would also be safer.”
ees and improved access to training modules. Future studies should expand upon sample size, as the low number of responses was a limitation of our study, as well as evaluate the new systems of emergency color code response that incorporate both the traditional color code format and the plain language approach.

References


Success in basketball has been a tradition at the University of Kentucky. For the security department of the University’s Healthcare Enterprise, this success has also meant dealing with the problems posed by student street celebrations as they affect the staff of the department and the operations of the university’s Level One trauma center.

Being a part of a university with a rich basketball history can pose challenges from time to time in the healthcare security realm. One might not make a connection between college basketball and a healthcare security operation, but at the University of Kentucky there is partnership in that we work alongside the UK Police Department. With the recent success of the University of Kentucky men’s basketball program, there is always the potential for large street celebrations to occur in multiple locations on our campus. The campus includes a Level One trauma center and a community hospital; therefore, our healthcare security operation was tasked with coming up with a plan to deal with these street celebrations. The first task at hand was having planning meetings with not only community leaders, but also with our own healthcare operations and discussing the impacts these celebrations could...
have on hospital operations.

CONTROLLING PARKING ACCESS FROM THE SWEET SIXTEEN TO THE FINAL FOUR

One of the first issues that we faced was the times that the NCAA games occurred. For example, some of the games occurred early in the day, during business/clinic hours. The City Police and University Police needed the top floors of our parking structures as staging/observation area for their operations, and these structures serve as the primary parking for our visitors and inpatient visits. Unfortunately one structure serves our Level One trauma center and the other serves our community hospital. We planned each game as the team advanced through the playoff brackets. We were able to avoid any great impact with patient visitors having a place to park. Our healthcare security team was tasked to secure and control access to the parking garage levels for each round of games starting with the Sweet Sixteen through the Final four games. As mentioned above these parking structures were used as observation points which means they were in right in the area where the street celebrations would take place. Also of importance and concern was to provide a secure environment for visitors entering the structures. This required the assistance of our healthcare security bike patrol.

KEEPING EMERGENCY ROOMS OPERATIONAL

A second issue was the need to secure and maintain the operational status of two emergency rooms, one being the Level One trauma center located across the street from what was expected to be the largest gathering area. Historically this has been the most violent and destructive area during these street celebration gatherings. Our second emergency room in our community hospital is located along a corridor which would see a large influx of people but has in the past not been violent or destructive. For both emergency rooms we provided additional staff for both inside and outside. We were also fortunate that we could station a sworn police officer inside both emergency rooms during the celebrations. The security officers stationed in
these locations did not report any increased calls for service or were they needed to mitigate any street celebrations type of incidents. There were very few patients transported to the emergency room during this time. One thing to note is we did ask the Level One trauma center administrators to notify all counties of the possible street closures and the increased pedestrian traffic due to these celebrations.

STAFFING, USING SOCIAL MEDIA, PROTECTING STREET SIGNS

A final issue was the actual staffing of so many additional posts while maintaining so called normal staffing. It is important to note that you have to have your additional staff on assignments as well as your normal operational staff for that period, but you also have to think about what to do if the incident goes past a typical shift. Come morning you will still have to staff your normal assignments and some of these officers may have been called in to address the incident. An issue that may come up with some security departments is the number of radios available to the officers. We are fortunate enough that we do not have to share radios and also have a few in reserve in case of radios getting damaged. One option we did consider was moving around schedules for our security shifts which are normally eight hour shifts to 12 hour shifts for those game days. The decision was made to maintain the current eight hour shifts and that worked for us.

Some of our other important issues that we had to consider were the public relations aspect of this incident being so close to our healthcare facilities. We had support from our public relations department in the hospital, but also had added support from the campus public relations department. We used social media to keep people informed and our campus and city police also monitored social media using software that alerted them of any talk of the different crowds around our property. We worked with our grounds and maintenance people to make sure that all removable items such as large trash receptacle and bike racks and even signage was removed if possible to make sure that none of these items were used to block streets
or create other hazards. With regards to signage, we did not remove stop signs or emergency directional signage but more of street signs only during the actual event. In previous years the city had to replace over 50 signs after the street celebrations due to their being pulled up and used to break other things and stolen.

**TESTING SECURITY’S RESPONSE TO CROWDS**

As it turns out the outcome of the final game did facilitate the dispersal of the crowds and their effect on our hospital operations. Looking back at this celebration, like many in the past, we were able to test several of our emergency plans to see what will work in the future. Our security team was able to test its response to large crowds in and around our hospitals and how we would maintain security and operations with these large street celebrations. It doesn’t take much imagination to change the scenario up to where you have a large crowd in and around your hospital due to and epidemic outbreak, or other situation that would draw potentially violent crowds. We were able to test our response with a mostly celebratory crowd. We were able to test our own resources both in personnel and equipment due to the large deployment of officers.

One area that was not tested and I must admit I am grateful we didn’t have to, is our ability to keep this type of presence for an extended period of time. Our emergency rooms were also able to test their ability to maintain operations and also prepare for a potentially large influx of walking wounded and decontamination due to the exposure to OC spray and other less than lethal projectiles. Although the success of our university basketball team on the court was not achieved this time, I do believe that our security team did put together a game plan that was successful.
Secure partnership: ENA, IAHSS leaders agree on need for continued team-up

Amy Carpenter Aquino

Reporting on a meeting between the presidents of ENA and IAHSS, the author describes a number of ways presented at the meeting in which security officers, ER nurses, and other staff members can collaborate to more effectively protect patients and staff from violence in the Emergency Department.

Safety in the emergency department is one of ENA’s top priorities, which is why the association has reached out to other organizations with similar concerns, including the International Association for Healthcare Security and Safety. After a joint meeting at ENA headquarters last summer, ENA and IAHSS leaders are discussing how the two organizations can continue their partnership into 2015 and beyond with the shared goal of protecting patients and staff.

“Everyone needs to feel safe—all staff, not just nursing,” said 2015 ENA President Matthew F. Powers, MS, BSN, RN, MICP, CEN, who oversees EMS operational and clinical services in his role as an emergency medical services battalion chief for the North County Fire Authority in San Mateo County, Calif., and as an emergency nurse supervisor for Kaiser Permanente-Vacaville.
“Patients, families and anyone else within the hospital need to feel safe.”

Although there were no formal plans in place when Powers spoke at the end of 2014, he emphasized the importance of partnership and communication among all departments when it comes to the issue of violence in the ED.

“When it comes to dealing with any type of violent behavior situations, there has to be a coordinated plan between hospital administration, the administration of the emergency department, all staff members—including contracted or hospital-managed in-house security,” Powers said. “Everyone has to have a plan, everyone has to be on the same page, as well as be able to drill together and practice for these situations.

“For example, if there were to be what we call a ‘takedown’ that would occur, that’s something that needs to be well communicated in the plan in advance, to protect the patient and also protect the staff. Communication is key.”

Marilyn Hollier, CHPA, CPP, director of hospitals and health centers security for the University of Michigan Division of Public Safety and Security, and the 2014 president of the International Association for Healthcare Security and Safety, said nursing is in a prime position to strengthen partnerships.

“Nurses have a big voice in the hospital; they’re the majority of the population, so there’s power in nursing,” Hollier said. “My perspective is that they should be partnering with IAHSS to make sure hospitals understand that security is a valued partner in the healthcare team.” When it comes to ED security personnel, Hollier noted the importance of hiring security officers with the ability to successfully comprehend the specialized training required in healthcare security, and security directors with professional certifications, such as the IAHSS certified healthcare protection administrator, or CHPA. “Healthcare security in and of itself is a specialization,” she said. “You can’t just walk off the streets and be a healthcare security officer because it’s a very complex and gray world. But a lot of hospitals don’t know that yet—they hire people that are not trained specifically to the nuances in a hospital,
or they’re more traditional-cop-focused, and that’s not successful inside a hospital. So I think that one of the ways we partner is by educating hospitals and C-suites on the value security brings.”

Both leaders agree that issues surrounding behavioral health patients offer great potential for further collaboration between nursing and security. The November 2014 incident in which a 68-year-old patient wielding a metal pipe was videotaped chasing and attacking several nurses in a Minnesota hospital—reportedly causing two nurses to be hospitalized with injuries—might have ended differently if there were early identification procedures and barriers in place, Hollier said. “That patient just couldn’t help himself, so that family and the staff are all victims here,” she said. “Hospitals are going to see more of that with an aging population.”

She described how the University of Michigan Hospitals program uses early identification as a tool for nurses. “We identify the patients, or their families, in the past that have been disruptive or have hit or pinched or injured a nurse, either through dementia or delirium…and they call security ahead of time.”

Security personnel partner with nurses in cases involving restraints and sitters, including identifying patients who require a higher-end sitter. The university system also uses a preferred assignment model that has been particularly successful, Hollier said. The officers’ primary work assignments are in the ED so they build relationships and become part of the ED team.

“My whole mantra has been about hiring highly skilled and trained security officers and providing ongoing training, but also about becoming that irreplaceable partner on the healthcare team and getting the community to understand that they have a role in keeping that hospital safe,” she said.

Powers suggested a tri-disciplinary approach, with emergency department staff, security and mental health staff working together to be able to understand the behavioral health and/or addicted patient and to establish team trainings for tactics such as de-escalation and determining hospital lockdowns.
Hollier said it was essential for all ED staff, from clerks through nurses, to be trained in non-violent crisis intervention training. Security’s expertise is also valuable in advising ED staff on proper security systems and proper service integration.

Powers said maintaining the momentum, perhaps with joint position statements or studies to establish benchmarking, will strengthen the partnership between ENA and IAHSS. “The most significant piece is that we all came to the table together to look at the areas that need to be improved regarding security systems across the U.S. while understanding our unique roles and challenges,” Powers said.
Violence in healthcare--one nursing student’s perspective

Michael S. D’Angelo, CPP

Seeking the answers on why so many nurses are leaving the profession in their first year on the job, the author interviews a former nursing student, now a clerical employee in his hospital, on the violence she experienced in her clinical career. Her answers, he concludes, pinpoint why nurses are leaving the profession and what has to be done to prevent a future “disaster” in healthcare.

For security managers working in healthcare, it has become commonplace to find your e-mail inbox flooded with articles and reports of workplace violence occurring in facilities across the country. The national statistics from almost all sources show continued increases in violent encounters. Type 2 of the FBI classification--violence against service providers perpetrated by clients (patients, families, and visitors against healthcare staff)--continues to rise at an alarming rate. More recently, the Occupational Safety and Health Administration released its new version of Guidelines for Preventing Workplace Violence for Healthcare and Social Services Workers. This document reveals that incidents of workplace violence in healthcare are still increasing. Over 70% of reported assault incidents stem from the healthcare and social services industries.

By now, most healthcare facili-
ties (HCF) have employed some measure of education, training, and awareness programs pertaining to decreasing incidents or properly responding to incidents of violence. Many organizations are bringing in professionals with well designed workplace violence prevention programs. Other hospitals are utilizing professionals within their organization to present and educate.

In our healthcare system, Baptist Health South Florida, we internally present a four-hour program entitled *Healthcare Workplace Safety; Recognizing and Responding to Aggressive Behavior*. Although the course covers many related topics, it has a concentration on the training of practical de-escalation techniques for healthcare staff. Like many presenters, I find that starting the class by sharing the alarming statistics is an excellent way to get the audience’s attention and to stress the importance of the proceeding program.

During a recent session of the program, while discussing a commonly cited survey that reveals 72% of nurses do not feel safe in the workplace and that 60% of new nurses leave the profession within the first year due to workplace violence, an attendee, Jessica*, instantly raised her hand. “He is absolutely right and I am living proof of the 60%.” She went on to introduce herself and tell me that she worked in a clerical position within our real estate acquisition department because of the workplace violence she experienced while in the clinical setting. She went to school working towards her BSN and also worked as a medical assistant at another organization’s clinic and hospital, but she left the clinical side of the profession in just over a year and a half.

What could an enthusiastic and obviously bright nursing student encounter in the workplace that drove her out so fast? Something powerful caused her to feel the need to validate the statistic. The classroom was not the setting to compel her to share her personal story. However, later that day I contacted Jessica. I wanted to know if she would feel comfortable sharing the details of her story with me. “I would be happy to. The statistic is scary and I know exactly why.” I went on to explain there would be tremen-

*Name changed to protect her identity
dous value in sharing her story with me, both for educating our fellow employees and hopefully to assist all of us in directly addressing the causes of this alarming statistic.

A STORY BEHIND THE STATISTICS

The following is my interview with Jessica, a medical assistant and nursing student who was driven out of the profession in less than two years due to workplace violence:

Q: Good morning Jessica, thank you for your time and candor on this very important topic. I think there is tremendous value in what you are about to share. When I mentioned the “60%” statistic, your face lit up and you immediately raised your hand, what compelled you to share?

A: The statistic is absolutely right and I lived through it. It needs to be talked about and it needs to be addressed or it will continue to turn people away from the profession.

Q: Tell me about your schooling and your start in the field.

A: I was attending a private nursing college and while going to school, I accepted a position with a local private clinic as a medical assistant. The clinic was not in a great area of town and treated a lot of indigent and low-income patients. The place also treated a lot of drug users and many psych cases. There was no real security or protection for the staff. Worse yet was the attitude of administration.

Q: What was the administration’s support?

A: None. Getting assaulted was part of the job! In one instance, I was taking vitals of a patient named Darwin who had an extensive psych history. In the middle of vitals, Darwin lunges forward at me and with both hands grabs me around the throat. As he is choking me he is yelling: “you are so beautiful.” I had to forcibly pry his hands from around my throat while trying to scream for help. Other staff members showed up and started to try and calm Darwin down. Management told me to calm down, take a break and have glass of water! No calling the police, no throwing the patient out, nothing! As I was taking a break trying to regain my composure, they allowed Darwin to continue treatment and see another medical assistant. I even
tried to talk to co-workers about the incident and they too acted like I was making a big deal out of something that happens all the time.

Q: You were assaulted. You were the victim of a crime. Nothing was reported and nothing changed in the clinic as a result?

A: Nothing at all. There were incidents of violence with other patients all the time. They never called the police about anything, never wrote any internal reports, and maintained the attitude that this is just part of our business.

Q: Obviously, this made you lose faith in your management’s support, but going forward, how did you now feel about coming to work?

A: I was terrified. Everyday I went to work expecting to be attacked. First thing I did everyday was check the patient roster for the day. If I saw Darwin was scheduled to come in, I was immediately upset. Even though they would not schedule him to see me, a few minutes before his appointment time, I would go out to my car and drive around the neighborhood in circles until his appointment was over. It was the only way I could deal with it. There was no way I could be in the same building as him. No way I could work and see him. I would not be able to function.

Q: And the only support from the clinic’s administration was to allow you to take a break and leave until he was gone?

A: That was it. My co-workers continued to blame me for making a big deal about it and actually accused me of bringing it on. They would say that because I was attractive and wore makeup, or styled my hair a certain way that I brought it on. I started to come to work with no makeup on, my hair a mess and trying my best to look unattractive. I did everything I could to not give off that impression.

Q: You made those changes, but you started to believe some of what they said?

A: I knew it wasn’t me, but I would try anything to avoid being attacked again.

Q: That was an absolutely toxic working environment. How could you continue to function and work in that atmosphere?

A: I couldn’t take it much longer and after a year and four months
I quit.

(About the same time as leaving the clinic, Jessica transferred schools to a local state university where she continued on with her nursing studies. She managed to secure a position with an area hospital’s cancer center while doing the clinical portion of her studies. Her position was on the overnight shift.)

Q: You mentioned to me that when you were working nights at the hospital, you also experienced workplace violence, but of a different kind. Tell me about that.

A: There was tremendous hostility among the staff. No one got along and some of the arguing got aggressive and often escalated to violence, but there was also hostility from patients and almost the same attitude from the administration. I was attending to a patient who noticed my tattoo (on the inside of Jessica’s right wrist is the Buddhist symbol for “Om,” the sound one makes when meditating) and immediately began screaming that she did not want to be treated by a terrorist and accused me of being Middle Eastern.

Q: How did the hospital’s management respond?

A: Again, it was me! They moved me to an administrative position behind a desk so I would not intimidate the patients!

(After less than six months in the clinical setting of the hospital, Jessica quit. Of even greater concern is she quit school and gave up completely on her dream of being a nurse.)

A: I always wanted to be a nurse. I loved the clinical and treatment side of caring for patients, but there was no way I was staying in that profession. The level of violence is ridiculous and the lack of taking it seriously by administration is insane! Management seems to only focus on the compassionate parts of patient care and ignores the risks and dangers to staff.

Q: What was next for you once you walked away?

A: I got a clerical job with Baptist Health South Florida in the real estate department. The attitude and support from the administration is very different here. Perhaps if I started my nursing career here things may have been different, but there is no way I would go back to patient care in the current state of things in the industry. I took a huge pay cut when I left nursing, but I
WHY THE ‘60%’ STATISTIC IS SO HARMFUL

The “60%” statistic is harmful in several ways. Obviously, losing nurses within their first year is costly to the organization that hires them. Additionally, with the nursing shortage in our country, holding on to qualified nurses is vital. If losing nurses within the first year is a tragedy, then losing nursing students before they even graduate is a pending disaster.

Although nothing Jessica shared with me is new or shocking to those of us in healthcare security, certainly some serious issues rise to the surface of the problem. None more concerning than a lack of concern from the leadership of healthcare faculties. We can establish all the prevention and intervention programs necessary to address the issue, but without internal support from senior leadership, significant change in trends will not occur. Statistics are attention getters, but far too often proactive change does not take place until a healthcare facility falls victim to a serious incident of workplace violence.

Top down buy-in can be demonstrated by “zero tolerance” workplace violence policies issued from the highest levels within an organization. That practice has to be followed up by strict enforcement of the policy and Human Resource Department’s immediate follow up with penalties (in most zero tolerance policy, an act deemed to be workplace violence results in termination).

The mindset that being assaulted is all “part of the job” for healthcare professionals must disappear from our culture. Assault, battery, and other acts of violence are crimes and in most cases warrant law enforcement involvement. Because they may take place in the healthcare setting is never an excuse for acceptance. Care, support, and counseling for victims of workplace violence should be part of any healthcare organization’s workplace violence prevention programs.

Lastly, although we are at the forefront of the epidemic, healthcare workplace violence is not a security issue. It is an organizational one.

References
Improving staff safety and the patient experience through redesign of security’s role in the emergency department

Drew Neckar, CHPA, CPP

A multi-pronged approach that provided training to ED staff so that they would be more comfortable in dealing with emotionally disturbed patients and which realigned Security’s role from patient observation to more of a response and support role has had positive results, according to the author. These include a significant improvement not only in staff’s perception of personal safety, and real monetary savings, but also in the perception of care by the patients themselves. The project has also resulted in a decrease in security officer time spent in patient observation, he reports.

(Drew Neckar CHPA, CPP, is Director-Security Services, Mayo Clinic Health System in Eau Claire, WI, and manages security for the System’s northwestern Wisconsin region facilities. He is a member of the ASIS International Healthcare Security Council and a former Vice Chairperson of the Upper Midwest Chapter of IAHSS.)
provided to mental health patients in the emergency department rather than increasing levels of security staffing levels and involvement in the emergency department.

HEALTHCARE FAILURE MODES AND EFFECTS ANALYSIS

Based on the survey responses, a multi-disciplinary team was formed with membership made up of front line employees and leaders from the Emergency Department, Behavioral Health, Security, Social Services, Nursing, and Quality Improvement Departments. This team used a Healthcare Failure Modes and Effects Analysis (HFMEA) methodology to quantify and isolate what issues could be driving the staff’s concerns.

The HFMEA methodology began with identifying and mapping 22 high level process steps for providing care in the Emergency Department for a patient who would be admitted to the inpatient Behavioral Health department. Once process steps were identified, each was evaluated for potential failure modes, or ways that the process step could result in a less than optimal situation. Each of the 322 failure modes identified was then evaluated for potential causes and rated on severity and probability to assign an overall hazard score to the failure mode. Those failure modes with a hazard score over a set threshold were then further evaluated for action.

The initial results of the HFMEA showed that the medical staff felt that in order to assure their safety additional security officer staffing should be employed in the Emergency Department. Appropriate levels would include one-to-one security officer observation with any patient deemed to present a risk of violence, and around the clock security officer presence in the emergency department’s waiting area.

Further analysis by leadership from the Emergency Department, Behavioral Health Department, and Security indicated that a possible root cause of the problem could be related not to having too few security officers, but instead to the comfort level of the emergency department staff in managing mental illness. While 27% of patients presenting to the emergency department had a behav-
### Example of a HFMEA worksheet

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Patient arrives in the Emergency Department</td>
<td>No Security Officer present</td>
<td>Security Officers busy with other ED patients</td>
<td>2</td>
<td>4</td>
<td>8</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Security Officers busy with in other areas of facility</td>
<td>2</td>
<td>4</td>
<td>8</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Security Officers not notified of patient arrival</td>
<td>2</td>
<td>4</td>
<td>8</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Security Officers responding, but not yet arrived due to large physical footprint of facility.</td>
<td>2</td>
<td>4</td>
<td>8</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td></td>
<td></td>
<td>No appropriate room available</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Only two rooms designed for high risk patients</td>
<td>2</td>
<td>4</td>
<td>8</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td></td>
<td></td>
<td>All ED rooms are full</td>
<td>2</td>
<td>4</td>
<td>8</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
</tbody>
</table>

The HFMEA methodology begins with mapping each step in the process that is being evaluated. Once process steps are identified, each is evaluated for potential causes, and each potential cause is scored as to the severity if it were to occur and the probability that it will occur on a 1-4 scale. Probabilities and severity are then combined to create a hazard score for each potential cause and causes with a hazard score over a set threshold are further evaluated for action.
A multi-pronged approach was developed that would be implemented by providing training to ED staff so that they would be more comfortable in dealing with emotionally disturbed patients and be more able to recognize and signs of incipient violence. This would allow for early intervention, re-align Security’s role from patient observation to more of a response and support role that would allow them to apply their specialized skills more appropriately, and to establish a Behavioral Health Liaison RN position within the ED to provide expertise.

REALIGNMENT OF SECURITY’S ROLE

During the FMEA process it was identified that while security officers were already spending nearly four thousand hours each year in the Emergency Department conducting one-to-one observation of patients. It had become so common for emergency department staff to see a security officer with a patient that some of them had begun to refer to patients who had presented in need of care for mental illness as “Security’s patients.” This was also reflected in complaints from patients who mentioned the perception that they were being “arrested” or that they feared that assumptions were being made about them due to having a uniformed security officer posted outside of their room based not on their behavior but only on their diagnosis.

In addition to these issues it was determined that in order to provide the level of security that the emergency department staff felt was needed to keep them safe while treating their patients, the Security Department would need to add minimally three security officers around the clock to their stuffing model, this would cost the organization over $630,000 annually.
Prior to project kick-off a survey was given to Emergency Department staff members to judge their perception of their personal safety and perception of their skill level when treating patients who were suffering from behavioral related disorders, the survey indicated significant room for improvement. After completion of the project a re-survey of ED staff also indicated an average twenty six percentage point positive effect on the scores of questions regarding perception of personal safety and feelings of competence in caring for patients suffering from a behavioral health diagnosis.
Based on these projections, it was determined early in the process that the model of making security officers responsible for the one-to-one observation of any patients deemed to be at risk for self-harm or harm to others was not sustainable or desirable. Alternatives were researched and it was determined that by shifting some of the responsibilities away from the Emergency Department Technicians, who were all licensed EMTs currently engaged in supporting the emergency department Registered Nurses, and onto the nurses that enough time could be freed up to shift the one-to-one observation duties onto these technicians.

This allowed security officers more freedom to respond where needed to de-escalate and manage potentially violent incidents both within the emergency department and in surrounding areas. To ensure appropriate response ability of the security officers who were no longer tied down performing patient observation, systems were put in place to allow emergency department staff to quickly notify security officers of developing situations. These systems included a personal duress alarm for each emergency department staff member and placing a handheld radio at the emergency department nurses’ station to allow for direct communication from the staff to the security control center as well as to the responding security officers. The personal alarm system that was chosen for the project utilizes infrared technology. It consists of Personal Infrared Transmitter (PIT) devices that all staff wear attached to their clothing, and infrared receivers throughout the area. Once a staff member either presses a button on their PIT or pulls it off of its lanyard, a signal is sent to the receiver and activates audio and visual alarms in the department notifying other staff and Security of the issue.

**TRAINING ED STAFF**

While all Emergency Department staff felt fully confident in their ability to deal with someone suffering from a heart attack or broken leg, many were not nearly as confident in dealing with non-physical symptoms of a patient suffering from mental illness. In fact when surveyed nearly sixty percent of Emergency Department staff said that they did not
Prior to implementation of this project in August 2011, Security Officers spent on average three hundred and thirty-three hours per month in the Emergency Department engaged in patient observation. The project was completed in May 2012, and three years post implementation that average has been reduced to sixty-six hours per month, a reduction of over eighty percent.
feel comfortable in their abilities to care for these patients. During the staff interviews and group discussions it was also became evident that staff did not feel fully comfortable in recognizing early signs of behavior that could lead to violence if not properly addressed and because of this were often categorizing all patients suffering from behavioral health disorders as having a high potential for violence.

To address these concerns and ensure that the Emergency Department Technicians were adequately prepared to take on the duties of one-to-one observation of the patients, the Security and Behavioral Health departments collaborated to provide training to Emergency Department staff in the basics of mental health diagnosis and appropriate strategies for working with patients who are affected by them, appropriate use of restraint and seclusion and the rules governing both, identification and de-escalation of potentially violent behavior, and self-defense techniques to prevent injury to them self or others in case a situation were to turn violent. Once they were equipped with these tools, emergency department staff were much better prepared to make risk based assessments of what, if any, preventative measures should be put in place with an individual patient.

THE BEHAVIORAL HEALTH LIAISON NURSE PROGRAM

Even with the additional training that was being provided to the Emergency Department staff it was deemed that it would be beneficial to have a subject matter expert with experience in mental health present in the emergency department during times when peak volumes of patients were being seen.

At the beginning of the project the emergency department was staffed with a social worker between the hours of eight o’clock in the morning and four o’clock in the afternoon. Interviews with staff showed that these social workers played a critical role in assisting with patients who were being admitted for treatment of a mental illness, and emergency department nursing staff relied on them heavily for their subject matter expertise. Unfortunately an analysis of volumes of patients being admitted for treatment of a mental illness showed that peak volumes of admissions were consistently presenting to the emergency department between the hours of two o’clock in the afternoon and two o’clock in the
morning, during the hours where there was no social worker coverage available in the emergency department.

It was decided that based on patient volumes, a subject matter expert in mental health was needed in the emergency department from when the social workers ended their day at four o’clock in the afternoon until at least two o’clock in the morning. After considerable discussion it was determined that this coverage would be provided utilizing a nurse with significant experience working with mental health patients. This nurse would be able to assist the emergency department nurses not only by providing mental health expertise, but also by beginning specialized mental health care earlier and working to facilitate the patient’s transfer to the inpatient behavioral health unit if appropriate.

RESULTS

Two years after implementation the project has resulted in significant improvement not only in staff’s perception of personal safety, and real monetary savings, but also in the perception of care by the patients themselves. The project has resulted in a decrease in security officer time spent patient performing observation from an average of 317 hours per month to a post implementation average of 66 hours per month, an 81% decrease, as well as a significant decrease in the number of incidents of assaults on staff perpetrated by patients. It has also resulted in speeding the throughput of patients from the emergency department to the inpatient behavioral health department, decreasing the average time a patient requires observation in the ED from an average of more than three hours to an average of slightly less than two hours, a thirty nine percent reduction.

A secondary, but even more important, benefit of this was seen in a significant rise in patient satisfaction scores for patients admitted to the inpatient Behavioral Health unit through the emergency department. Within one year of project implementation, patient satisfaction scores rose from the 70th percentile to the 90th percentile nationally. After completion of the project, a re-survey of ED staff also indicated an average 26 % positive effect on the scores of questions regarding perception of personal safety and feelings of competence in caring for patients suffering from a behavioral health diagnosis.
Preventing child sexual abuse in youth-serving organizations

Norman D. Bates, Esq., Christine Army, MA

Managers of youth-serving organizations like health facilities should be more aware of the many problems associated with child sexual abuse, according to the authors, whether they be in hiring or dealing with potential offenders, or in treating or interviewing victims. They point out that offenders may include family members and other visitors as well as patients.

Child sexual abuse (CSA) is an insidious crime that can destroy the lives of innocent children and leave their families devastated. The topic of child sexual abuse is, at best, a difficult subject to discuss and at worst, a horrifying one. Child sexual abuse has been defined as:

"Child sexual abuse involves any sexual activity with a child where consent is not or cannot be given. This includes sexual contact that is accomplished by force or threat of force, regardless of the age of the participants, and all sexual contact between an adult and a child, regardless of whether there is deception or the child understands the sexual nature of the activity. Sexual contact between an older and a younger child also can be abusive if there is a significant disparity in age, development, or size, rendering the younger child incapable of giving informed consent. The sexually abusive acts may include sexual penetration, sexual touching, or non-contact sexual acts.
such as exposure or voyeurism.”

INTERPRETING THE DATA

Estimating how many children are being or have ever been sexually abused is problematic. Some of the challenges that are faced include: inconsistent state definitions of child sexual abuse, under and non-reporting, a variety of report receiving/data collecting agencies and how the data is reported.

1. Inconsistent State Definitions of Child Sexual Abuse: There is no single definition of child sexual abuse used currently. States vary in what age is considered a “child” as well as who can legally be held responsible for child sexual abuse.

2. Under and non-reporting: Many cases of child sexual abuse are not reported right away and some are never reported. Therefore, the actual number of children who are or have ever been sexually abused is currently unknown.

3. Report Receiving Agencies: Depending upon how a state defines child sexual abuse, reports will usually be reported to either local law enforcement or Child Protective Services. However, many instances of sexual abuse never reach these agencies and are dealt with internally by the organizations and/or individuals involved.

4. Data Collecting Agencies: There are a number of agencies that collect data on child sexual abuse. The National Child Abuse and Neglect Data System (NCANDS), the data collecting system of the National Data Archive on Child Abuse and Neglect (NDACAN), gathers information from participating CPS agencies. However, they do not collect data from local law enforcement. This means that current data collecting systems only capture a portion of the total incidents of CSA.

5. How the Data is Reported: Understanding the scope of child sexual abuse means taking into account both prevalence and incidence rates. The number of child sexual abuse cases will be reported in one of two ways: incidence or prevalence. “Incidence rates are based on how many children were abused in a single year. Prevalence rates are based on a lifetime or a full childhood, such as what percentage of all children were ever abused.”
THE SCOPE OF THE PROBLEM

1. Intra-and Extra-Familial Sexual Abuse: The reality of child sexual abuse is that most offenders are known to their victims, including relatives and family members. It is estimated that approximately 90% of juvenile sexual abuse victims know their perpetrator in some way. However, the first gap in research and statistics of child sexual abuse is the challenge of categorizing offenders of child sexual abuse. Part of this can be attributed to the inherent complexity and nature of human relationships. Individuals can have family members, relatives, biological and non-biological parents/relatives, close friends, friends, acquaintances, friends of the family, trusted persons, known persons, and strangers. It is no small feat to attempt to classify each case of sexual abuse into one of these categories, and therefore the categories are often condensed for purposes of simplicity. Some studies condense the categories of offenders to “known” versus “stranger”, while others attempt to elaborate and separate offenders into categories of relative/family member, acquaintance, and stranger.

The lack of uniformity about how to characterize offenders leads to poor estimates of the perpetrator data for child sexual abuse. Within the data analysis, how to distinguish a trusted coach who is a “friend of the family” from a worker at a local youth organization, who does not share a similar relationship to the family, remains an enigma. Because most child sexual abuse occurs within the family, traditional research may place less importance on the other categories of victim/offender relationships. This may be why the data for intra-familial child sexual abuse is more thorough than that for extra-familial child sexual abuse.

2. Disclosure of the Abuse: In addition to facing categorization difficulties, data regarding child sexual abuse is also skewed because of delayed disclosure or non-disclosure. Consequently, the exact number of children who are sexually abused annually is difficult to estimate. Yet, according to the Darkness to Light organization, “even if the true prevalence of child abuse is not known, most professionals agree that there will be 500,000 babies in the US this
year that will be sexually abused before they turn 18 if steps are not taken to prevent it.”

While the concept of non-disclosure poses a problem similar to that of delayed disclosure, the term “disclosure” itself lacks a clear and concise definition among researchers. Disclosure in this publication means the victim making sexual abuse public.

One of the main factors in whether children decide to disclose incidences of sexual abuse has primarily to do with who they are reporting it to and how likely those people are to believe what the children are saying. Parents should therefore maintain and create comfortable communication between themselves and their children. Studies have shown that “more than half of all child abuse incidents are never reported because the victims are too afraid or too confused to be able to report their experiences.”

3. Limited Prosecution of Offenders: Another challenge to the accuracy of child sexual abuse rates is the limited prosecution of child sexual abuse cases. For example, arrests are made in only 29% of the cases reported to the police, with arrests being made more often in incidents involving older children (32%). Arrests are made in only 19% of cases involving children under the age of 6. In many cases where arrests are made, there is no prosecution.

Another possible reason for a case to not be prosecuted is the retraction of the accusation. Due to the pressure and encouragement of some adults, there are situations in which children will take back their accusations. There are a number of possible reasons why parents or guardians would pressure children into retracting their statements. One of the main reasons is that parents are concerned that their child would suffer more if made to go through an investigation and trial. This is often done on “behalf of the child,” so as not to put them through additional trauma.

Another reason for there to be no prosecution may be a lack of sufficient evidence. It is for this reason that reporting, interviewing, and investigative protocols are crucially important. They may be the difference between prosecuting the crime or not.

OFFENDER CHARACTERISTICS

Offenders may have some similar attributes and grooming pat-
terns. However, there is no profile, per se, of a typical abuser. There are no standard characteristics that are predicative of an offender of child sexual abuse. Hearing the word “profile” can turn into prejudice and assumption of guilt on certain persons. While there may be common traits, not everyone that has one of these traits (e.g., not being married) is by any means automatically an abuser.

‘Grooming’

“Grooming” is the process of how offenders make initial contact with the intended victims and the methods they use to develop a relationship with children in an attempt to normalize their behavior. It is a premeditated behavior intended to manipulate potential victims into complying with the sexual abuse.

VICTIM CHARACTERISTICS

Similar to there being no definitive “profile” of an offender, there is also no “profile” of a typical victim of child sexual abuse.

However certain characteristics may make some children more vulnerable to abuse or to an offender. Jerry Sandusky targeted young boys in the Second Mile charity organization which was geared towards at-risk children living in disadvantaged circumstances.

One method used to help understand victimization is to gather information directly from the individuals who sexually abuse children regarding how they choose their victims. This perspective is invaluable to future procedures and policies to prevent child sexual abuse. One offender commented, “You can spot the child who is unsure of himself and target him with compliments and positive attention.”

Guidelines

Specific components to the prevention of child sexual abuse within youth-serving organizations include appropriate pre-employment practices, the training of personnel, protocol on the interaction of personnel and youth participants, and the physical design elements of a facility that can act as a possible deterrent to potential abusers.

PRE-EMPLOYMENT SCREENING AND BACKGROUND INVESTIGATIONS

The first step in developing a program to reduce the risk that a youth-serving organization will
hire a sex offender is to establish a comprehensive pre-employment screening program for all employees, volunteers, and contract employees who may have contact with the children being served by the organization.

While management for the YSO may not have direct control over the background checks conducted of contract employees (e.g., security personnel, cleaning staff, kitchen staff, etc.), specific requirements for those checks can be addressed in the contracts between the organization and contracting agency. It is important that management of a YSO establish minimal background check requirements for all staff, regardless of their employment relationship to the organization.

Legal Issues
There are several legal issues that employers need to consider. Every state has different laws and frequently, certain federal laws will also affect the way organizations can conduct background investigation. Prior to implementing a program, have the proposed program reviewed by an attorney experienced in employment law.

The most common legal issues encountered in pre-employment screening programs include:
• Negligent hiring liability
• Employee privacy rights
• Employment discrimination and violations of federal and local state statutes

Negligent Hiring Liability

Negligent hiring is defined as the failure of an employer to exercise reasonable care in selecting an applicant in light of the risk created by the position to be filled.

Negligent Hiring Versus Traditional Employer Liability

Negligent hiring is easily distinguished from traditional employer liability. The difference is that traditional employer liability is actually vicarious or direct liability for the actions of employees while they are working on behalf of the employer. Negligent hiring is liability imposed for the employer’s own negligence in the selection process.

In the traditional form of employer liability, the legal doctrine of respondeat superior operates on the principle that employers are responsible for the actions of their employees when tasks are performed on behalf of the employer and in the employer’s general interest.

If the employee committed a
harmful act outside the scope of employment and not to the benefit of the employer, the company may not likely be responsible. If the harmful conduct clearly falls outside the scope of employment, including acts that could not be reasonably anticipated by the employer, then the doctrine of respondeat superior may not apply and no recovery would be made against the employer.

Employers are not always exposed to liability just because they failed to check an applicant’s background. Liability results when an adequate and legal investigation would have revealed a background logically connected to the wrongful conduct. For example, the failure to discover that an applicant was convicted of child molestation, when he is allowed to work in a day care center for children could result in liability should he subsequently molest a child at the center.

**STEPS OF AN EFFECTIVE SCREENING PROCESS**

**Corporate Policy Statement**

Managers need to establish an organizational position statement on the subject of criminal history checks which will indicate that the organization does check this data and the importance of such investigations.

**Risk Associated Positions**

Management needs to determine which job positions represent a potential risk to others, should these employees be able to use their position to cause harm. Different job positions within a company or organization can pose a variety of risks by virtue of the work or tasks performed. While there are certain categories of jobs that include inherent risks (e.g. working with children) most positions may not be that obvious. The employer must look at what exposures are created when the employee has “unsupervised access” to vulnerable people or dangerous objects.

“Unsupervised access” is the key in understanding how one determines whether or not the position sought to be filled represents a risk. Using this criterion, managers should write down each type of unsupervised activity/access that each position represents and ask themselves the following: If we hire a person with serious criminal conviction(s), especially for violent crime, are we placing our clientele at risk?

**Risk Factors**

A common example of a position
of “risk” is created by the unsupervised access to a variety of vulnerable individuals or circumstances creating an opportunity to cause harm. “Risk” is not a function of the employee’s wages, job title or skillset. Consider an employee’s unsupervised access to the following as examples:

- Children
- Master keys
- Elderly persons
- Persons who are disabled
- Private homes
- Patients - mental and/or physical illness
- Weapons

The following is a representative list of risk factors related specifically to child sexual abuse within youth-serving organizations. Note that the emphasis is on “unsupervised” access to children in a variety of ways.

- Unsupervised contact with children
- Transportation of children
- Long term contact with children in live-in situation
- Extreme physical exertion in a remote setting with children
- Visit to children’s homes
- Helping children change clothes, bathe, or with other personal activities
- Coaching sports in which physical contact between adult and child is routine
- Delivery of meals to children’s homes

SUPERVISION OF STAFF AND VOLUNTEERS—POLICIES AND PROCEDURES

Creating, adapting and maintaining a Policies and Procedures Manual in youth-serving organizations is a component of providing safety and well-being to children as well as employees and volunteers. Many YSOs have already implemented and documented in their employee handbooks such things as “Code of Ethics, Standard Care Practices, and Guidelines for Conduct.” Also, YSOs should check with their local state legislature to ensure that all state mandated policies are being followed.

Adult/Child Interaction

Adult and child interaction policies are important to preventing child sexual abuse. They also help to reduce suspicious or inappropriate behavior between adults and children.
Adult and child interaction refers to how many adults are required to be present with a single child. These guidelines help limit the frequency of situations where potential child abusers are left alone with a child or children.

**SUPERVISION-PHYSICAL DESIGN OF FACILITIES**

There are two general components to the supervision of staff and volunteers at a YSO. The first, discussed previously, is the establishment of policies and procedures that are designed to regulate the interaction between children and adults.

The other component to supervision is the design of the facilities and a variety of physical security measures available to YSO’s. In the 1980’s the architectural profession developed a concept known as Crime Prevention Through Environmental Design (CPTED). The basic premise of CPTED is to design a facility—both the interior and exterior—in such a way that the ability to observe areas and define physical boundaries is maximized. Designing spaces that are open and visible through the facility ensures that individuals with a propensity to commit child sexual abuse do not feel comfortable pursuing their abhorrent behavior.

Organizations should realize that many of these design features rely on the already established facility. A number of youth organizations take up residence in older, brick buildings, which can pose a number of detrimental design flaws including a lack of sufficient lighting, isolation spots, closed or locked doors, hallways empty of supervision or staff, a lack of visibility into rooms or areas and restrooms that may be located in isolated areas. Older buildings also struggle with a “front desk” area which would enable supervision over who enters and exits the facility and their whereabouts when inside.

**CONCLUSION**

In conclusion, while many of the YSO’s have undertaken a number of steps to keep the children safe, there are many such organizations that have not faced the facts about the profound risks to children that exist every day.

(Note: This article is an excerpt from “Preventing Child Sexual Abuse in Youth Serving Organizations”. A copy of the full publication is available online at www.liabilityconsultants.com)
To treat and cure them, you must first keep them safe
Dr. James D. Blair, FACHE

The author maintains that Accreditation in Healthcare has failed to keep us safe from the threats of more frequent and robust natural disasters, more virulent and drug-resistant biological agents, and increasing levels of man-made violence in healthcare, including active shooters, terrorist threats and workplace violence. This article focuses on natural disasters and biological agents. For other articles in the series, go to www.chcer.net

We live in an era of increasing uncertainty and danger from more frequent and robust natural disasters, more virulent and drug resistant biological agents, and increasing threats of internal and external violence. According to the National Oceanic and Atmospheric Administration (NOAA), the number of billion-dollar weather related events in the last 35 years has grown from a low of zero in 1987 to a high of 16 in 2012. Examples of healthcare failures to protect stakeholders these events are legion. Katrina was the worst in our history with over 300 inpatient lives lost from preventable causes, such as lack of electricity to maintain air conditioning and life-sustaining medical equipment due to flooding of primary and back-up generators that were below the flood plain.

(Dr. James D. Blair, FACHE is president and CEO of the Center for Health Care Emergency Readiness [CHCER], Nashville, TN.)
JOINT COMMISSION REPORT UNDERSCORES HOSPITAL NON-COMPLIANCE

A recent Joint Commission Online Report provided an overview of the most challenging Accreditation and Certification Requirements for the first half of 2014. According to the report:

“The Joint Commission collects data on organizations’ compliance with standards, National Patient Safety Goals (NPSGs), the Universal Protocol for Preventing Wrong Site, Wrong Procedure, Wrong Person Surgery™, and Accreditation and Certification Participation Requirements to identify trends and focus education on challenging requirements. These data also help The Joint Commission identify risk areas to highlight in the Focused Standards Assessment (FSA) process.”

Among the findings in the report related to hospital readiness to address emergency requirements associated with these increasing natural disasters, there was a whopping 58% non-compliance rate for “Manages Risks Associated with Utility Systems” within Critical Access Hospitals, while within all Hospitals the non-compliance rate was 53%. These numbers underscore the problem and beg more urgent action on the remediation of these deficiencies. We would suggest much more aggressive oversight in these areas.

JOPLIN AND SANDY: ELDERLY PATIENT CASUALTIES

Despite high levels of self-reported Emergency Management readiness at the State and Local levels in Joplin, Mo., after-action reporting showed that Long Term Care providers were not invited into the Community Disaster Management Planning Process. In the massive 2011 Joplin tornado disaster, 11 residents of a single long term care facility lost their lives.

In a scathing Office of Inspector General (OIG) report in September 2014 concerning the preparation and response to Hurricane Sandy, results showed that 89% of the hospitals surveyed reported “Critical Challenges” such as electrical and communications failures and that most had been cited for three years before the storm. Half experienced electrical
failures, the cause of hundreds of lives lost seven years earlier during Hurricane Katrina, and the exact same problems for nurses, including lack of training to manually operate automated IV drips and respirators when machines lose power.

It seems the only consequences for not fixing the deficiencies was another round of billions in taxpayer dollars to repair the hospitals, and a lot of backslapping about how well hospitals responded to the crisis. One of the evacuated hospitals that flooded out and had to be evacuated, NYU Langone, was advertising itself as one of the safest hospitals in the country within months of reopening. If the hospitals were accredited and cited for being non-compliant in Emergency Management for the exact reasons that caused the failures, what is the purpose of Accreditation, and where is the accountability?

Despite the claims that there were no healthcare-related deaths as a result of the storm, a study of 610 long term care (LTC) residents from a Sea Crest Nursing Home in Brooklyn revealed that within three months of evacuation, 125 had died. These were a fraction of the 5,500 LTC and Adult Home residents evacuated during the storm. In addition to the tornadoes, flooding and super-storms, drought, ice storms and wildfires have become increasingly prevalent in the last decade due to climate change.

The healthcare industry’s “sicker and quicker” approach to admit and keep acute cases while discharging them as soon as it is safe, exacerbates this danger of the disasters; more fragile patients in the ICU and NICU are likely to need evacuation in the worst case scenario, and these patient rely most on life-sustaining equipment, driving the need for adequate electricity, food, water and medicine during emergencies. The most fragile patients were the ones evacuated down dark, flooding staircases during Sandy. Although none have officially been counted among the fatalities from the storm, a follow-up of those patients might reveal higher morbidity or worse outcomes than others, especially among the elderly.

**INCREASINGLY VIRULENT BIO-AGENTS**

Many experts believe the great-
est threat to the human race is the possibility of a global pandemic sweeping across borders faster than it can be contained. More virulent and drug resistant biological agents are proliferating around the globe and are able to move quicker than ever before with the billions of international travelers. H1N1, H5N3, SARS, MERS, HEV68, Marburg, and Drug-resistant TB have all emerged as international threats within the past few years.

The US is seeing a resurgence of measles, a disease that was essentially eradicated with the help of strong Public Health programs to vaccinate children. The 2009 H1N1 response was completely inadequate in containing the spread, and the latest OIG report concerning Epidemic Influenza Preparedness is titled: “DHS Has Not Effectively Managed Pandemic Personal Protective Equipment and Antiviral Medical Countermeasures.” Major findings include that the national stockpile of 200,000 respirators to be distributed in a pandemic have exceeded their warranty dates, as has all the hand sanitizer and a majority of the anti-viral vaccines and medications. As seen in a Frontline Slide Show, the growing number and types of drug resistant bacteria is alarming, as is the loss of efficacy in existing antibiotics and lack of new antibiotic drugs in the pipeline. For a deeper look at this serious public health issue see the video http://video.pbs.org/video/2365104403/ It shows how NIH brought a drug-resistant-bacteria into their premier hospital and were unable to control it or eradicate it from the premises. As we address the challenge of Ebola inside our borders, we need to keep in mind that the NIH and CDC are our main line of defense and they are already stressed to capacity dealing with these other challenges.

THE EBOLA CRISIS

According to Reuters, Emory University had serious issues dealing with the hazardous waste associated with treatment of the two Ebola patients they treated. The report said their HAZMAT waste partner refused to handle the material and a deal had to be brokered by CDC and the waste disposal contractor as infectious waste piled up for six days inside the hospital. This is an excellent example of how even the most
“ready” facility in the country can be vulnerable to unforeseen and unplanned difficulties. From an accreditation perspective, the above-mentioned Joint Commission Online Report, *42% of Critical Access Hospitals and 50% of Hospitals are non-compliant* in the area of “Reduces the risk of infections associated with medical equipment, devices, and supplies.” This begs the question of whether the hospitals which failed are still operating and treating patients with public money; we know it is extremely rare for a hospital to lose their Accreditation and Certification as the result of poor performance in an Accreditation survey. As if these numbers were not alarming enough, Infection Control Today released results of a survey that says registered nurses overwhelmingly believe we are unprepared to treat Ebola. Key Findings:

- More than 60 percent of RNs say their hospital is not prepared for the Ebola virus.
- 80 percent say their hospital has not communicated to them any policy regarding potential admission of patients infected by Ebola.
- 85 percent say their hospital has not provided education on Ebola.
- 30 percent say their hospital has insufficient supplies of eye protection (face shields or side shields with goggles) and fluid resistant gowns.
- 65 percent say their hospital fails to reduce the number of patients they must care for to accommodate caring for a “isolation” patient.”

As with lack of preparedness for natural disasters, without serious consequences or accountability for that kind of performance, we will not be ready to deal with a large scale epidemic regardless of what officials say to the contrary.
Blue ribbon panel hears how to respond to biological and chemical threats

Anthony Kimery

This article reports on the final session of a Panel of former officials and Congressmen of the Clinton, Bush, and Obama administrations formed to recommend changes to U.S. policy and law to strengthen national biodefense while optimizing resource investments.

If America were to be beset by a biological or chemical weapons attack, who would be in charge of responding? According to the consensus of the post-9/11 Commission Blue Ribbon Study Panel on Biodefense arrived at during its fourth and final meeting last week, “The federal government doesn't have a good answer to that question.”

"The last thing we want to do is experience a successful bio-attack in the United States and not be in a position to respond," said former Rep. Mike Rogers (R-Mich.). "It's hard to get people's attention about biological and chemical threats that can't be seen or touched but have devastating consequences nonetheless. We have to make this a public health issue."

Following Rogers's testimony, panel co-chair Tom Ridge presided over five discussions that explored methods of re-
sponding to biological and chemical weapons attacks—and the "leadership vacuum" that plagues response efforts—especially the response to a large-scale, mass casualty bio or chemical attack. "The federal government has stated that a public health disaster or pandemic is one of the top strategic threats our country faces," said Dr. Kenneth Bernard, a former biodefense official in the Clinton and Bush administrations. "Yet, we were still largely unprepared for the Ebola outbreak this year. We're not managing our leadership properly."

Three veterans of the Clinton and Bush administrations spoke of a "balkanized" response to biological and chemical threats. They called for future presidents to make biodefense a bigger priority—and to delegate authority to a White House official to coordinate the activities of federal agencies.

The Blue Ribbon Study Panel on Biodefense will identify and recommend changes to US policy and law to strengthen national biodefense while optimizing resource investments. The panel will produce a report that will: assess ongoing efforts; articulate actions to improve the nation's ability to prevent, deter, prepare for, detect, respond to, attribute, recover from and mitigate biological and large-scale chemical incidents; and identify near and long-term actions by current and future Congresses and presidential administrations. The Report of the Blue Ribbon Study Panel on Biodefense will be issued later this Spring.

‘AMERICA HAS NOT LEARNED FROM PAST TERRORIST ATTACKS OR NATURAL DISASTERS’

In his keynote address, Dr. Irwin Redlener, Professor of Health Policy and Management at Columbia University, lamented that America has not learned from past terrorist attacks or natural disasters. "We haven't defined what it means to be 'prepared' for a major disaster," he said. "America remains more vulnerable and less resilient than it should be. Instead of engaging in random acts of preparedness, we must be proactive."

"Biological and chemical threats are among the most sinister our nation faces," Ridge said. "Terrorist groups have voiced their desire to obtain and use biological and chemical
weapons. The Ebola crisis revealed significant gaps in US public health and medical preparedness. We must consider our current ability to defend against such threats and provide for the health and welfare of our citizens."

*Homeland Security Today* has consistently reported on the nation’s ill-preparedness for a catastrophic biological or chemical attack—the former of which carries with it the worst case scenario—beginning with the inaugural issue's report, *The Trauma in America's Trauma Care*.

"In the past 13 years and with a seemingly endless parade of domestic disasters that continue to challenge our health care response (in some cases to the point of collapse and beyond), it still appears our health care infrastructure writ large has failed to embrace the readiness mission. And it’s not for any lack of important and knowledgeable voices who continue sounding the klaxon alarm regarding the risk we face in perpetuating the health care community’s failure to embrace the preparedness paradigm," wrote CBRN/Public Health Preparedness Contributing Editor Dr. Peter Marghella in his June/July *Homeland Security Today* cover report, *When the Crossroads of Health Care and Public Health Never Meet*.

Former director of the New York State Office of Emergency Management, Marghella was a career Naval officer who served as a plans, operations and medical intelligence officer in the Navy Medical Service Corps, retiring as director of medical contingency operations for the Office of the Secretary of Defense. Previous assignments included chief of medical plans and operations for the Joint Chiefs of Staff, chief of medical plans and intelligence for the US Pacific Command, and chief of medical plans and intelligence for the Office of the Chief of Naval Operations. His national-level planning credentials include authorship of the nation’s first Catastrophic Incident Response Plan and the National Smallpox Response Plan.

**LESSONS LEARNED BY THE NEAREST TRAUMA CENTER TO THE WORLD TRADE CENTER**

"Just one year after the Al Qaeda attacks on Sept. 11, 2001, David Campbell, the former CEO
of St. Vincent’s Medical Center in New York City, was invited to address the plenary session of the annual American College of Healthcare Executives (ACHE) Congress in Chicago. Shortly after the attacks, Campbell had written an important article about the experience he and his staff encountered as the closest Level I trauma center to the World Trade Center site. In that article, Campbell detailed lessons learned which were intended to help health care organizations become better prepared for dealing with the aftermath of mass casualty events,” Marghella wrote.

“In addition to discussing those important lessons learned for hospital organizations as a result of the historically unprecedented attack, Campbell issued a clear warning to the assembled health care executives: ‘9/11 should be considered a catastrophic casualty anomaly, in that there were more fatalities than there were survivors requiring critical care support. Had the reverse been true, it is arguable whether the health care infrastructure of New York City and its surrounding environs (i.e., surrounding states) could have absorbed the casualty load and provided adequate resources to support the victims.’”

Marghella said, “Campbell went on to opine that the findings of the 9/11 Commission would have been radically different if such an important critical infrastructure and key resource sector had suffered a catastrophic failure in its capacity to support the incident management mission of such a nationally significant and, at the time, historically unprecedented event. He further argued that this recognition called for enhanced disaster planning at the organizational level of all hospitals, and that it is vital that it is coordinated into community-wide planning for all major hazard events.”

In her Pulitzer Prize-winning book, Five Days at Memorial: Life and Death in a Storm-Ravaged Hospital, Dr. Sheri Fink “takes readers on a nightmarish journey through the ravages of Hurricane Katrina in 2005, and the consequences related to health care organizations having failed to embrace the preparedness mission and the role that they would take on in sustaining community-based resilience,” Marghella said. He emphasized though that readers “can only be left shaken and
bewildered relative to how we continuously fail to take on the hard lessons for adequately managing future catastrophic and mass casualty events. Health care professionals who read Five Days at Memorial should quake with fear that they might be faced with the same life and death decisions because their organization’s leadership decided to give short shrift to the issue of preparedness in advance of the panoply of hazards we now face as a nation.”

HAVE THE 21ST CENTURY WAKE UP CALLS BEEN SNOOZE ALARMS?

As Dr. Irwin Redlener, one of the nation’s most vocal proponents of health care and public health preparedness—recently noted at a conference sponsored by The Atlantic on public health emergency preparedness, “The wake-up calls,” of the first 14 years of the 21st century “have all turned out to be snooze alarms,” Marghella noted, adding that, “In an interview with Homeland Security Today, Dr. Len Singer, medical director of the Healthcare Preparedness graduate program at Boston University Medical School, was even more forceful about the situation. ‘We have to stop living in a fantasy world and face reality,’ he said.”

Marghella said, “Singer agrees with the contention that the common denominator to all disasters is human casualties, and, inasmuch, no other critical infrastructure and key resource sector resource will be at the epicenter of our readiness capacity.”

“We can have all the best wishes in the world and all the best plans in the world,” he said, “but unless we have buy-in by the proper stakeholders”—hospital and healthcare system leadership—“we are in no better shape that we were pre-9/11.” Redlener “also believes we are not going to see any substantive changes to our medical and public health response capacity until we begin to approach preparedness differently,” Marghella wrote.

PUBLIC HEALTH VS. PRIVATE HEALTHCARE PREPAREDNESS

“There is no CINC [Commander-in-Chief] of preparedness” that can function as a cabinet-level lead for domestic preparedness and response—with all of the attendant (and required) control of forces that are medically-centric in their response capacity, Redlener said. “Once the bell goes off and we’re in a disaster, the barriers between
health care and public health should disappear, as [the incident management prosecution mission] becomes a jurisdictional governmental responsibility," Singer said. "Right now, if the private health care system collapses, the public health system—underpinned by government—must be prepared to step up to the plate."

"But neither the government is as prepared as states or local jurisdictions think it is, and private sector assets expect them to be available," Marghella warned.

"In an attempt to ready the public health care sector in a post-9/11 world, the newly formed Department of Homeland Security (DHS) in 2002 decided to treat the public and private health care sectors as similar in terms of emergency management requirements. In retrospect, it might not have been the best approach," wrote Jim Blair in his Homeland Security Today report, Forcing Emergency Preparedness on Health Care. "The private sector has a long history of avoiding and delaying regulation, i.e., maintaining inventory of personal protective equipment, seismic upgrading in earthquake zones, installing redundant utility systems in flood zones, securing radiological materials vulnerable to theft and in-place detonation, among other things." A 50-plus year career in progressive levels of responsibility within the private, public and military health care sectors, including serving as a CEO at military hospitals, Blair has spent 15 years in preparing health care organizations to meet their expected role in the nation's strategy for CBRNE and all-hazards preparedness.

"While federal resources could be (and were) mandated to achieve a higher level of readiness, the remaining 90 percent of the nation's public health care sector could not be enticed or coaxed into following suit," Blair wrote, pointing out that, "Public health sector emergency readiness became a hot potato issue, passed back and forth among DHS, Department of Health and Human Services and Centers for Medicare & Medicaid Services (CMS)—with no ultimate authority to enforce a standard of preparation. The private sector dragged its feet, and even DHS could not entice hospitals to adopt suggested guidance, despite the private sector's receipt of federal grant programs and resources."
Budget reductions vs. loss of security training

John M. White CHPA, CPP

During the past few years many healthcare security budgets have been cut, and with that, budget lines for ongoing training of officers and other employees have been reduced, the author reports. Stressing that such training is essential to a hospital's protection, he presents in this article ways to achieve cost savings that will keep your training program alive and well despite budget cuts.

Over the last several years there has been a lot of budgeting pressures placed on healthcare facilities. As a result many service lines have seen their budgets either frozen or reduced in an effort to ensure fiscal responsibility throughout the healthcare organization.

Many times, when budget cuts are under consideration, administrators seem to be looking first at non-patient care services, such as Security. One could argue that Security is part of the patient care team. However the fact is that not all hospital administrators see it that way. In many cases the reductions in budgets have resulted in reduced security staffing levels, either by not filling vacancies as they arise or by force reduction through layoffs.

Another means by which to reduce budgets is to look closely at other expenditures such as equipment, overtime and training budget lines. Unless your department has an extensive array of se-
curity technology, your budget line for those resources may likely already be marginal at best.

Finally, as we all know, staffing dollars, those monies spent on man-hours, account for the majority of your budget expenses. Although we have seen a steady rise in violence in healthcare over the years, the reality is that healthcare organizations have had first to respond to the ever-shrinking reimbursement dollars, and non-patient care departments are likely to take the first and largest hits when budgets are affected. In some cases, unfortunately, we may be giving them cause to believe that because perhaps we are not ensuring that our security program’s effectiveness is known to our administrative teams.

In summation, regardless of the reasons why security services may not be considered part of the patient care team, we must continue to ensure that we are bringing value to our organization, and that we insist on security training for both security staff as well as all other hospital staff members.

SECURITY TRAINING VS. SECURITY CULTURE

Security training is a critical part of the foundation of any organization’s security program, and therefore its security culture. This is regardless of whether we are talking about the security staff’s training or that of the organization’s other staff members. Both are important parts of the security culture, and if one is absent or underutilized, an organization’s risks and liability may be elevated.

In the world in which we live and work in, if your organization is not providing some type of security training to staff, you may find that during an emergency your staff may react in a variety of ways. Absent any consistent training or written instruction that requires staff to respond in an approved manner to a security incident, the actual results of their responses cannot be foreseen. In other words, if employees do not know what they are supposed to do, you as a security professional cannot anticipate with any degree of confidence how they will react or respond. Thus, there are general risks your organization faces as a result of insufficient training.

The risks can be reduced provided there is a trained security presence working at all times, and their numbers are sufficient to ad-
dress all security incidents independently. However, the reality is that not all organizations have a trained security staff on duty. In addition to that, we as security professionals often view all company employees as an extension of the security department regardless of the number of officers we might have on staff. Basically we often rely on all employees to be our eyes and ears because we as security professionals know we cannot be in all places at all times.

KEYS TO A SUCCESSFUL SECURITY TRAINING PROGRAM

Most large businesses provide security awareness training to all new hires at orientation, and some types of businesses take it even further by providing annual refresher training of all staff. However, like many other parts of the corporate world, the emphasis on security training may not be uniform across the board, and in some cases it is dependent on budgets or the corporate culture. A larger number of businesses will likely have security information of some type included within their “Employee Handbooks” if they provide one, yet there is no means or process in place to ensure that staff actually reads any of that information, and in many cases staff is not evaluated for proficiency with regard to the information.

Commitment

A successful security program, whether or not you have a security department, must have the commitment of all staff and other users such as visitors, patients, tenants, vendors, contractors, students, faculty, and so on depending on your type of facility. A security awareness program is essential and should become a fundamental element of every employer’s daily operation and business model. Employees, management, and other personnel that either work or live onsite need to become aware of their roles and responsibilities with regards to security. Implementing a security awareness program is an important step in reducing liability concerns and identifying security issues at the earliest possible stages, giving you time to make adjustments as a mitigation strategy. So when it comes to assessing the security training of an organization, there are numerous
things to consider and evaluate.

Maximizing Training Budgets

As mentioned earlier, training budgets, including travel to trade conferences, have been cut in many cases and in some organizations those budget lines have been eliminated. Does this mean that we can just forego ongoing training? The short answer should be no, but the reality is that that does happen.

Let’s assume that your training budget has been reduced substantially, and yet you still need to provide training for your security officers. So how can you provide such training with little or no budget dollars? At this point you need to look at all available resources both within and outside your organization.

Internally you should look at departments such as Risk Management, Human Resources, Legal, Compliance, and Safety to mention a few options. Each of these departments can provide training programs, and in many cases do so with little or no costs to your department.

When looking externally, look to the local police and fire departments. For example, your local police can provide training on gang violence, workplace violence prevention, officer safety, defensive tactics, and so on. Your fire department can provide fire suppression training using fire extinguishers and may be able to provide basic training regarding entering confined spaces, of which many large medical centers have at least a few spaces that would meet this definition. Again, in most cases there may be no cost for this training with the exception of the fire extinguishers used, which can be equipment from your facility.

One of the largest expenses for training is staff’s payroll to attend the training. However, with a little effort and strategic planning you can reduce the budget for such expenses and possibly eliminate overtime altogether.

Faced with little or no budget allocations for training, some medical center security managers have been tasked with training staff without utilizing overtime. Now when you are talking about an operation that is 24/7, and you are not allowed to utilize overtime to get staff trained, you really have to get creative. Creativity comes with making schedule ad-
justments for security officers, which will include changing either days off or shifts, or a combination of both. You will also need to plan for a few different training sessions in order to get all staff through the training. You may be thinking that it is impossible to train your officers without using overtime, but it can be done with planning and coordination.

Value Added Security

As we in healthcare security compete for the shrinking budget dollars, we need to ensure that our program’s value is apparent throughout the organization. On more than one occasion I have heard healthcare executives state that there are very few security concerns within their organization. However, when talking to the security staff it becomes clear that that is not the case. The difference in the two viewpoints is that security deals with security incidents daily, yet no one is keeping the senior team informed and therefore they are not aware of the value of the security program.

There are many ways in which to ensure that the value of the security department is well known and appreciated throughout the organization and it is incumbent on security management to ensure that that is the case.

One way is to bring value to your security program is to provide security awareness training for staff and volunteers of your organization. In many cases you are probably doing some security awareness training to all staff in new employee orientation, and if you are lucky you are providing them annual training other than the standard online training that many healthcare organizations have switched to in order to save money.

Another option is to look at short training sessions during meal breaks. In some organizations they refer to these as brown bag training sessions. Brown bag training sessions or seminars are generally speaking a training or information event during a meal break. The term "brown bag" often refers to the sack lunch meals that are either brought by the attendees or provided by the employer. Brown bag training seminars will normally run for 30-60 minutes and provide information to attendees in a strictly voluntary and informal setting,
and each session is often followed by a discussion of the topic along with a question and answer session.

A third option is to provide information sessions and security training to community members and even employees during the evening hours. One medical center did this very successfully and as a result they found that staff would remain after work to hear the speakers on their own time. In addition, members of the community would show up in large numbers to hear the speakers and find out how they could improve their personal security. This type of training cost the medical center nothing, and yet the medical center received excellent feedback from both the public and staff.

IN CONCLUSION

Let’s face it. Many of your departments are facing budget cuts now or have faced budget cuts in the past. When it happens, you may be responding by telling your administrator that the security services are needed and should not be cut or eliminated because there is an ongoing risk associated with workplace violence or other security issues. The fact of the matter is if you are having those conversations now, where you are trying to justify your department’s budget, it may be too late.

Basically, the administrative team has made the decision to make cuts because they felt it could be done with little or no impact on the organization. So why did they come to that conclusion? Each case may be different but in several of the cases that I have reviewed it was because they were not aware of the value that security brought to the organization overall.

Over the last six to eight years many healthcare security budgets have been reduced, and in some cases entire departments have been eliminated. Many of the healthcare security management professionals that I have spoken to about this have agreed that the often-stated reason given to them was that reimbursement dollars are down, and cuts need to be made to non-patient care departments.

When pressed further, they also agreed that they could have done a better job of demonstrating the value of their program to the organization. A few even stated that
they thought that the organization knew all of the good things that the security department was doing, but in the end they realized that that was not the case.

The end result is it all comes down to how well you manage your program and how to ensure that the value that your security department is bringing to the organization is well known. When and if the time comes to make budget cuts, and if it means reducing budget lines such as training, you have to look at ways to do so and yet still keep the training at the highest level possible. Looking internally and externally for potential costs savings is one way to keep your training program alive and well despite budget cuts.

Finally, we all know that staffing costs are often our largest expense when it comes to training, so get creative with your scheduling of security officers so that you can reduce or eliminate a large portion of overtime dollars spent on training. This may be an inconvenience for some if their days off are changed for one pay period, or if they are required to change shifts for a couple of days, but in the end it may be enough to keep your security program alive and well even if your budgets are reduced.
An alternative view in the development of healthcare security metrics

Anthony Luizzo, PhD, CFE, CST, PI (ret. NYPD) and Bernard J. Scaglione, CPP, CHPA, CHSP

The use of security metrics, according to the authors, is a much better way of improving the acceptance of security awareness programming. However, they report, healthcare security budgets continue to be based largely on the intuition of company management. In this article, they present a number of metrics that speak the language of clinical and administrative personnel and give security professionals more effective ways to validate the business of security to the C-Suite.

(Anthony Luizzo, PhD, CFE, CST, PI (ret. NYPD) is a member of the Board of Advisors of Vault Verify, LLC, and Stage One Screening, LLC. He was the former corporate director of loss prevention for the NYC Health and Hospitals Corporation. He was the first elected Eastern Region Governor of the Association of Certified Fraud Examiners and is the President Emeritus of the New York Chapter of Certified Fraud Examiners. He is a frequent contributor to the Journal of Healthcare Protection Management.)

(Bernard J. Scaglione, CPP, CHPA, CHSP is the director of healthcare security services for G4S Secure Solutions. He has 30 years of experience in the healthcare field: including a Master’s Degree from Rutgers University School of Criminal Justice. He presently serves on the board of IAHSS and is the past chairman of the ASIS International Healthcare Council. He is a frequent contributor to the Journal of Healthcare Protection Management.)

WHY METRICS ARE NEEDED IN SECURITY

In an October 15, 2013 article by Scott Greaux featured in PhishMe.Com, “Use Metrics to Measure and Improve Security Awareness,” while discussing the overall importance of using metrics to improve security awareness, the author states that most security awareness programming fails to gather and/or use metrics as part of its protection mosaic. Greaux goes on to discuss the importance of gathering as much information as possible about an institution’s services so that appropriate metrics can be developed and applied to properly meet todays and tomorrow’s challenges.

In “Persuading Senior Management with Effective, Evaluated Security Metrics” published by the ASIS Foundation in 2014, the report summarizes the need for effective metrics as follows: “Security metrics support the value
The use of metrics to evaluate the effectiveness of healthcare security services and staff has been widely debated. Several security organizations, including the International Association of Hospital Security and Safety (IAHSS) have conducted surveys and studies to determine which metrics work best in order to evaluate a given service. To date however, no real consensus has been obtained on what works best. On the contrary, many different ideas have been brought forth and many different types of metrics are used by healthcare organizations.

Oftentimes, most security executives rely on individual security expertise when developing metrics. These metrics are understood by the security professional but have not gained ground outside of the healthcare security field. Consultants and senior executives alike have not seen real value in security metrics, and in general dismiss them as being ineffective or demonstrating no real value to the evaluation process. In “Persuading Senior Management with Effective, Evaluated Security Metrics” the authors discuss the criteria for evaluating an effective
security metric. They state that a security metric should be reliable, have validity and have generalizability. They should operationally demonstrate cost, timeliness and be manipulative. They should be strategic demonstrating return on investment, organizational relevance and be easily communicated.

IDEAS THAT DESERVE CONSIDERATION

PRODUCTIVITY INDICATORS:

Clinical Length of Stay/Discharge Rate. On the surface, it appears that there is no real value in the use of length of stay or discharge rate when evaluating security services; and in general, that is true. Alone, this metric holds no real value in the determination of service relative to the security of patients, visitors and staff. But, when we compare these rates with the long term evaluation of incident rates or calls for service, we can compare the effectiveness of monthly or quarterly service by monitoring its highs and lows. This metric works because when length of stay is low, and discharge rate is high, the number of patients and visitors within the hospital is greater. In theory, the number of incidents and calls for service should be accordingly higher as well. When compared over time, the security department can demonstrate value by showing a decrease in the incident rate when more people are using the hospital. Comparing security-related incident rates or calls for service with length of stay or discharge rates illustrates the effectiveness of security services as compared over time and to other hospital departments that utilize the length of stay metric in evaluating service.

Square Footage. Although it is clear that square footage alone is not a valuable metric in the evaluation of security services, it is a statistic that many consultants rely upon in evaluating healthcare support services. For security services, the amount of square feet does not wholly determine the amount of staff necessary in order to provide a safe and secure environment. Still and all, this statistic can be useful in demonstrating the effectiveness of services. The value of using square footage as a metric is its acceptance with consultants and the C-Suite alike. This metric demonstrates its value
when compared to security data over time, or with other facilities of similar square footage. If the call for service rate is higher in comparison to other facilities, or increases over time, the metric demonstrates an increase in the level of service and suggests the need for more staff. If the incident rate is lower over time, or lower than other similar institutions, the security service is efficient in its delivery.

**WORKLOAD/CALLS FOR SERVICE**

"Touches." Generally, security departments report the number of incidents that occur, the number of patrols conducted, or the number of visitor passes dispensed. These statistics, no matter how they are presented, demonstrate the amount of work that the security department produces in a given time period. It does not show the value of the service provided. However, if the data collected shows how many times the security department interacts with patients, visitors and staff, coupled with the type of interaction furnished, then the security department can demonstrate its value and effectiveness based upon the patients, visitors and staff served. So, what metric is important in the evaluation of calls for service? *Ergo, then "Touches" is the metric that should be used!* Touches are not the number of patrols conducted, or the hours that an officer held a post, it is the interaction with the customer and the results of that interaction. Reporting the number of times security accompanied and/or assisted staff to their designation, provided directions or escorted them to their vehicle, is a more definitive evaluation of the service as compared to the number of patrols conducted or the hours an officer stands post. Many times security departments will document and report the number of doors they unlocked or the number of doors that were found unlocked and/or opened. With respect to these types of assignments, opening a door for a staff member is a touch. In this case, a staff touch can be both a positive and negative metric. Having a high number of touches to assist staff in a non-patient related way may not be seen as a positive metric when it is compared to patient and visitor touches. Comparing the number
of staff touches with patient and visitor touches can demonstrate the need to reduce staff interaction or increase patient and visitor interaction, translating to less door openings and more facility patrols.

**Near Misses.** The term, "Near Miss" is used in the healthcare setting to indicate the intervention or discovery of an incident or event that *could have been adverse*, but was averted. This concept can be used in healthcare security since it is more readily identifiable than a door found open, a behavioral health patient that tried to leave the hospital and was stopped, or the continued denial of an access card being presented to a storeroom or high security door. In lieu of reporting the number of doors found open, reporting a near miss related to a purse left unattended or a computer that could have stolen is a better, more understandable, metric. Not reporting the patient who almost left the hospital or the employee who is continually trying to access a door that they have no access to, negates the effectiveness of the security services provided to the institution. A near miss is an evaluation tool to which risk management, nursing and administration can relate.

**Interventions.** An intervention is a term that is used in the healthcare profession generally in the behavioral health arena. An intervention is a planned or unplanned interaction with a patient or client because of negative or potentially negative behavior. A patient restraint is an intervention; a patient watch is an intervention, a disruptive patient or visitor is an intervention. An intervention is a metric that can describe aspects of the execution of the security operative’s job that is not demonstrated by reporting basic workplace violence. Using interventions as a metric demonstrates actions taken to improve a declining or detrimental situation, and can be used to categorize the workload conducted by security staff in the prevention of violence within the hospital. This phraseology helps behavioral health administrators better understand the use of this metric by security and can provide a more defined application of security services.

**Staff Configuration/Work Force Management.** Staff configuration and/or work force man-
agement is the evaluation of staffing requirements and the costs associated with labor and other expenses, and are another metric that can be used to evaluate the effectiveness of security services. Generally, the security professional sees work force metrics as the cost by officer post or hours worked, two metrics that provide little insight into the financial value of security services as seen by the fiduciary administrator. In finance, the value of service is determined by the expense or the cost compared to patient care data or industry known metrics.

As such, in order to show value within financial metric circles, expenses should be compared by square foot or discharge rate. Comparing labor expenses or overall security expenses with square footage or discharge rates alone has no real value in determining the effectiveness of security services; but when compared over time or with like facilities, these metrics can demonstrate the value of security services over time. These metric measurements speak the language of the fiduciary aficionado. Experience demonstrates that the best metrics to use in fiduciary-related situations varies from entity to entity. Besides labor or expenses compared to square footage or discharges, financial data should be determined based on exceptions. In finance, exception reporting paints a true picture as to the state of expenses and overages that plague budgets. So, items like overtime, sick time, injury time off, accidents or breakdowns in vehicles and extra training are all examples of exceptions that influence budgets.

Other Metrics. From a programmatic perspective, the best metrics for security executives in the healthcare environment to employ are those metrics that hospital administrators know and understand. These may include: demographics related to employment/background checks, equipment outages, emergency responses, and policy and/or procedural violations. Finding the appropriate metric to exploit is limited only by the security administrator’s imagination.

CONCLUSION

Metrics are an effective way to validate the business of security to the C-Suite. By speaking the
language of clinical and administrative personnel, metric use and evaluation can better position the security department in the evaluation of services and its value to the organization. Beyond simply using metrics, it's imperative that a dashboard be developed to appropriately monitor and evaluate whether programmatic standards and metric applications are within acceptable, defined compliance standards. A dashboard consists of a series of graphs or data points presented on a single sheet of parchment, or on a computer screen that furnishes a clear picture of the task at hand. Applying effective mathematical metric measurements gives the security professional the capability of deciphering adverse incidents before they have an opportunity to adversely impact the intuitional setting.

Selected Bibliography

Although there are a number of best practices, guidelines and other resources available to assist security professionals in crafting an effective healthcare security program, the author says, there is a pressing need to transform existing standards and other reference materials into a consolidated format to meet specific needs. In this article he demonstrates how merging these seemingly incompatible requirements into a manageable system of assessment and program validation can become a reality.

Healthcare is one of the most highly regulated and scrutinized industries, and for a very good reason. The outcome of healthcare services, after all, directly impacts the health and well-being of its clients and customers. Similarly, healthcare security is highly regulated from a wide assortment of agencies, all reviewing differing aspects of the profession and its impact on patient care. For example, in the US, OSHA (Occupational Safety and Health Administration) focuses on the safety of the healthcare workers themselves, while CMS (Center for Medicaid/Medicare Services) has its focus on the patient. Add to this volatile mix any number of additional regulatory agencies, each with their own specific agendas and standards, and one can easily appreciate the complexity that a modern healthcare security prac-
tioner must contend with.

TRANSFORMING
MULTIPLE GUIDELINES
INTO CONSOLIDATED
FORMATS

While this may seem an impos­
sible task, there are certainly a
significant number of best prac­
tices, guidelines and other re­
sources available to assist us in
crafting an effective healthcare
security program. The IAHSS
(International Association for
Healthcare Security and Safety)
and ASIS (American Society for
Industrial Security) offer a wide
variety of reference materials as
well as invaluable networking op­
portunities for information shar­
ing and lessons learned, but much
of this information does not exist
in formats that lend themselves as
consolidated assessment tools. In
healthcare, as with many other
businesses, we have an increased
need to create documents and
spreadsheets to track a number of
indicators. These can range from
a simple inventory of equipment
to the tracking of the number of
incidents for any given location,
time frame or type of event. With
this high demand for metrics and
an assessment of the current state
of readiness of your organiza­
tion’s security program, the ques­
tion becomes: can we repurpose
existing guidelines, standards and
other disparate reference materi­
als into tools with which we can
validate our existing processes
and identify opportunities for im­
provement?

The issue comes down to a) tak­
ing the time to re-invent the wheel
or b) to transform existing stan­
dards and other reference materi­
als into a consolidated format to
meet a specific need. With ever-
dwindling resources and increas­
ing time restraints, one should
always opt for re-purposing exist­
ing information when possible.
Not only can we reduce the cre­
ation time, but we already have
industry standards that have been
created by regulatory authorities
to guide us. Creating and using
information that reiterates and
supports existing best practices
show a consistency for your pro­
gram and the healthcare security
industry as a whole.

TRANSLATING A
SECURITY MANAGEMENT
PLAN INTO A CHECKLIST

For example, the IAHSS pub­
lishes operational and physical se-
curity guidelines for healthcare security professionals in order to assist them in meeting and exceeding current regulatory requirements when it comes to the safety and security of patients, visitors and staff in the hospital environment. These guidelines include categories detailing program administration, departmental operations, investigations, emergency management, staff/patient services and physical security considerations, to name a few. Taken separately, each one of these guidelines works well in educating the security practitioner in a particular facet of their overall program, but none are optimized for use as a consolidated, easy-to-use assessment tool. Considering that these guidelines have already been categorized into logical sections, based upon subject matter, it is a fairly straightforward task to transform them from academic reference into a practical tool with which to evaluate existing processes and procedures.

By taking the existing IAHSS guideline regarding program administration and the development of a Security Management Plan, you can take the various steps outlined in this guideline and translate them into a checklist with which to inspect your own security program. This can be done in a variety of formats, but for ease of use we have found that by using and electronic spreadsheet, we can further automate the task by creating drop-down columns to easily record elements of performance, findings, actions required, persons responsible and progress status should improvements be required. Per the IAHSS Guideline, some of the elements of a Security Management Plan should include the following, each of which can be measured independently as part of the entire Security Management Plan review process:

1) **Security program mission statement**
2) **Statement of program authority** (e.g. an organization chart depicting reporting levels)
3) **Identification of security sensitive areas**
4) **An overview of security program duties and activities**
5) **The documentation system in place** (i.e. records & reports)
6) **Training program for the security staff and all other staff**
7) **Planned liaison activity with local public safety/other HCFs**
as appropriate

8) Security organizational chart

9) A copy of the most recent SMP annual program evaluation report and plan for improvement

By placing these questions in an assessment tool format, you can quickly determine if the element exists, if it is sufficient and up to date or who is responsible for mitigation and in what time frame. In reviewing element 1 above, the first question is 'Does a Security Program Mission Statement exist?' If not, then this will have to be assigned to a responsible party for creation and a deadline for completion established. If one does exist, is it current and does it meet the needs of the existing program it is intended to describe? What about element 3, 'The Identification of Security Sensitive Areas?' Experience has taught us that being overly descriptive with such areas can result in unwanted scrutiny from regulatory surveyors; however a complete lack of documented security sensitive areas can likewise appear unusual. In this case, a properly formatted assessment tool can provide the means to quickly examine the current list of such areas, make a determination as to their number (too many, too few or none at all) and create a mitigation plan and assign responsibility for resolution. Such details, when reviewed in a uniform and objective manner, make it easier to evaluate existing security program elements and identify regulatory gaps and opportunities for improvement.

DEVELOPING A MASTER ASSESSMENT TOOL

Another benefit of using an electronic spreadsheet format is that multiple regulatory standards, guidelines and best practices can all be translated and compiled into readily identifiable worksheets as part of a large, master assessment tool that is easy to maintain and navigate. This would be a living document as the very nature of its contents is constantly changing to meet the evolving needs of the healthcare industry, due to legislation, litigation or lessons learned. Other considerations are to color code those items which are requirements versus expectations, so that the "Must Haves" are distinct from the "Should Haves" or the "Like to Haves". Typically a
“Must Have” will have consequences should it not be met. “Should Haves” are those items that are considered best practices when feasible and resources allow, but do not result in negative consequences should they not be met. “Like to Haves” are just that and are typically used to demonstrate your security program’s best practices to others. By creating assessment tools from legitimate regulatory and industry standards, security practitioners can be assured that their program assessment is unbiased and objective based upon known and accepted practices from professionals in their industry. Such details are very important when using these tools as a validation for existing program resources or for justification when requesting additional resources to meet regulatory expectations.

Due to the multifaceted nature of both healthcare and security, when they are combined the result is a labyrinth of sometimes conflicting regulations, which somehow must be met and compliance demonstrated on a regular basis. By translating current reference materials into a consolidated, easy to use format, the task of merging these seemingly incompatible requirements into a manageable system of assessment and program validation can become a reality. By sharing the creation of such tools with other security professionals in a multidisciplinary and collaborative environment, we can all work together to increase the body of knowledge and promote uniformity in the application of industry guidelines and best practices. We all share the same regulatory requirements that must be met, so why should we not create and share the tools with which to meet them?
The employment interview is critical in hiring security and safety personnel who will perform up to expectations and strive to help the organization move forward, according to the author. In this article he presents a philosophical and practical approach to the hiring process that is best suited to meeting those goals.

For as long as I've been a manager, I've always believed and shared with my staff several principles that are part of my work ethic and values that I live by. One of those beliefs is that I only look as good to others as my staff will allow me to look. Their performance is a direct reflection of how I've managed, trained, supported, and enabled them to perform.

My goal is to apply my abilities, personality, work ethic, and management style in a manner that supports and encourages my employees. My objective is to provide them with appropriate training, proper equipment, and the support that they need so that they can demonstrate a performance that is positive. If your employees are appreciative of their employment and the opportunities that come with it, they will approach their responsibilities with the same initiative and eagerness. If they are doing a great job, it is a direct reflection that they have been given what they
need to do so. Employees that are engaged will often work with compassion and feel connected to the company. Your efforts should continuously encourage a sense of belonging. They will demonstrate initiative, innovation, and strive to help move the organization forward.

Conversely, if your employees are not provided with the appropriate training and proper tools they need to effectively do their jobs and remain safe, their talents will not be demonstrated and their initiative will diminish. No individual in any occupation wants to feel unsafe or be placed in harm’s way. I think this is especially true in healthcare security. If my employer did not provide me with the necessary training and tools to assure my safety, I believe I would surely be inclined to find an employer elsewhere that would. It should be obvious that you and your employer don’t want to waste valuable time and resources on turnover—rehiring, replacing, and re-training security staff that have very marketable skills. If an employee’s performance is poor or even failing, this too can be a direct reflection that they have not been given what they need to succeed.

The increasing occurrence and complexity of security and safety related issues, threats, risks, and liability strongly indicate that an effective security and safety program has become a business imperative. This is mission critical. It’s understood that the performance of your employees is often a direct reflection of what you have, or perhaps have not, provided for them. Selecting and retaining appropriate, skilled, educated and knowledgeable staff are key for business and security and safety program success. High caliber and talented individuals that strive to consistently develop their skills and increase their value to your organization and to your customers are your most important resource.

FINDING OUT WHAT THE APPLICANT IS SEARCHING FOR IN AN EMPLOYER

Constructively remain cautious of the ambitions of the applicant. Make an effort to determine what the applicant is searching for in an employer. You may consider questioning why the applicant wants the position that they have
applied for. Try to understand what is motivating the applicant for the position. Question what the anticipated longevity of the applicant would be. Answers to these questions may provide you with valuable insight that will help you with your hiring decisions. There are plenty of studies and research that provide data related to the various personas of those in position of employment are seeking. Although this type of information can certainly be useful in helping to determine if an applicant is profiled as a leader, follower, mentor or student, who is any better to ascertain if the individual is a good fit for your organization but yourself?

You want to consistently strive to recruit the absolute best employees for your organization's needs. You want talented employees who fit the organizations culture and strategic plan. Your recruiting strategies are critical in attracting these skilled and talented individuals. The objective of the hiring process should be to attract and identify the individual who has the best mix of skills, education, attributes, and experience for the available job.

DEMONSTRATING WHY THE APPLICANT SHOULD WANT TO BE PART OF YOUR TEAM

Successfully and effectively recruiting security and safety staff is your opportunity to solicit and show an applicant that your organization is stellar and one that is ranked high in many regards. Recruit a potential employee that would be proud to be part of your team, one that would be very appreciative of the opportunity to be an employee of your organization. You should indicate to the applicant as a potential employee that you demonstrate a substantial role in the training and development of staff, leaving no doubt that this is considered as a high level value to your security and safety program. At the same time, this lets the applicant know what the expectations of you and the employer are as well. The applicant should see up front that you promote a positive image to all guests, patients, employees, physicians, volunteers, and contractors.
DETERMINING IF THE APPLICANT WOULD BE A GOOD FIT WITH EXISTING SECURITY AND SAFETY PERSONNEL

The obviously fundamental requirements and appropriate qualifications, experience, and education should be what developed into the applicant interview process thus far. Not to be forgotten or discounted are the applicant’s ability and traits regarding excellent written and oral communication skills, ability to understand instructions, how well they can respond to inquiries, and how well they can prepare and complete a report. Equally important is whether the applicant presents as one that would be a good fit with existing security and safety personnel. Is there a sense of camaraderie with the applicant personality and the culture that is already in place? Is the applicant able to verbalize how they can appropriately intervene and deal with confrontational situations? Can the applicant verbalize how they are skilled in providing excellent customer service to the guests of your facilities? Ask the applicant to explain how they are qualified to make the right decision, at the right time. Ask the applicant to provide an example of how they once helped someone in need of assistance. Imperative is the knowledge and use of personal computers, and a strong willingness to work with technology in all facets of the position. Seek the applicant that has had some past stability. Really examine their past achievements, and evaluate how appropriate and relevant they may be to the position at your facility. Similar to education, some training and achievements may only be indirectly relevant or parallel to the needs of the open position being applied for, or may not be helpful at all. Do applicants present as though they would be capable of handling a dangerous situation?

MAKING CLEAR WHAT ARE YOUR EXPECTATIONS

This approach to recruiting and hiring well educated, experienced, and appropriately trained individuals is the beginning critical component of an effective and successful security and safety program. Retention of those skilled, professional, and high performing staff is just as critical.
Retaining employees is a charge of appropriately placing them into the best position for their abilities. This is also inclusive of consistently and continuously providing effective and appropriate training, education, and instruction. Develop methods to manage, coach, and offer your assistance to keep the highly effective and innovative security and safety employee satisfied. Make sure they continue to remain as appreciative of the opportunity and their eagerness to succeed as part of your security and safety team continues. At the same time, never neglect or underestimate the underperforming or low-performing staff. Question if these individuals may be in the wrong job. Evaluate whether you have provided specific and clear requirements and expectations so the individual knows what your expectations are of them. Unhappy, underperforming staff can drain the energy from talented, skilled, and high-performing staff members, even if they are new employees.

Consider why the applicant would desire and choose your organization as their next employer. Why would they want to work for you? Review what the candidate for the position has to offer, but what they may expect from you as the employer as well. There are numerous hiring and employment variables related to age differences, demographics, and even the current economic status of your particular geographic area. These variables may drive the direction of the interview, defining if your organization is presented as the candidate interviewer, or the interviewee. Despite these variables, always give consideration to the applicant’s potential for your organization, and how much of that is related to how well you have presented your organization and yourself to the applicant.
The prevailing opinion that excessive turnover of security staff is a negative and that little turnover is a positive, is not necessarily a correct one, according to the author. Either one can produce higher costs and lower program effectiveness, he says, recommending a "middle of the road goal of controlled turnover."

Security staff turnover is a significant factor confronting security staff management for most healthcare security programs. The term "staff turnover" is, more often than not, viewed as a negative aspect of security operations. There is, however, a flip side to this issue of management that may have a positive effect on the quality of security services being provided. The pervasive issue of staff turnover is an issue that should be addressed regardless of the in-house or other contract staffing model. Each organization needs to examine the turnover issue within its own operating system and community characteristics. A well-managed degree of security staff turnover is essential to a sound and efficient security program. It is the extremes of too little turnover, or too much turnover, that may be detrimental to properly achieving organizational objectives.
THE EFFECTS OF EXCESSIVE TURNOVER

The effects of excessive staff turnover are often more apparent to the organization than too little turnover. When there is excessive turnover the two major consequences are generally lower program quality along with higher new staff processing and training costs. In addition, there are increased scheduling challenges, rescheduling administrative time and often dissatisfaction of current security staff.

Measuring Experience and/or Training Costs

A major factor in security program quality is the productivity of the individual security officer. Productivity, aside from the officer’s personal desire to do a good job, emanates from experience in handling security activity that arises in the specific operating environment as well as knowledge of the physical plant layout and general policies of the organization. Experience in handling security incidents and even routine activities is the area that generally takes a good deal of time to create what we often call “a seasoned officer.” The desired amount of experience and/or training required cannot necessarily be measured in terms of a given time frame. It is more appropriately measured in the degree of complexity, and diversified types of activity/incidents in which the officer is directly involved. Again, the cost of new officer training is moderated by the quality and experience factor possessed by the new officer. On the other hand, learning the layout of the physical plant and grounds, as well as general policy and procedure, can be learned in a relatively short period of time. It may well be that pre-service training of new officers be individualized, rather than a specific duration of pre-service orientation and training, and be tailored to the personal attributes of the trainee. A well-structured competency training format, along with perhaps a field training officer acting as mentor/coordinator can appreciably shorten the pre-service training period of time. A field training officer function can produce a certain consistency of protection services.

Properly Reviewing Turnover Rates

In reviewing and analyzing staff
turnover, it is an error to view turnover in terms of a percent. Turnover should properly be reviewed in terms of the effect on the program not in terms of a number. As an illustration, let us assume that General Hospital and Memorial Hospital each experienced a 100 percent turnover of security personnel in the past year. General Hospital was generally recruiting new security officers who had little experience in health care security, while Memorial Hospital was able to recruit and hire new officers with a good deal of positive health care experience. In this illustration the negative effects of poor program quality and high training cost were abated, or minimized by, Memorial Hospital. Thus, the effect of a 100 percent turnover rate at Memorial Hospital had considerably less negative impact on cost and service than the same 100 percent turnover rate at General Hospital. As a side note, some organizations wrongfully view police experience in the same light, or even higher, than healthcare security experience. Required re-training of the experienced current or former law enforcement officer may well require more training time and cost than the applicant with at least a modicum of understanding of the healthcare environment and general principles of protecting an organization.

**TOO LITTLE TURNOVER: NOT NECESSARILY A BENEFIT**

Just as excessive turnover can produce a higher cost and lower program effectiveness—too little turnover can produce these same factors as well as creating an environment that fosters limited program innovation and little advancement opportunity. The higher costs from too little turnover are created by higher wages and benefits—not from training costs. As a general rule, program cost of too little turnover is far greater than the cost of training new officers in programs with high turnover. Another effect of too little turnover is program quality. Program quality may suffer due to the patterned, lethargic, and complacent activity that can often result from the failure to bring “new blood” into the security operational program.

Security staff turnover must also be viewed in terms of positions,
including the number of supervisory positions, turning over. Let's illustrate by again looking at a specific scenario. A 100 percent turnover rate of parking lot security officers in one year is completely different from the same 100 percent turnover rate of shift supervisors. The loss of investment, and program continuity, is relatively small in the category of parking lot security, compared to such factors when viewing the turnover of security operation supervisors.

FORMULATING A ‘CONTROLLED TURNOVER’ PLAN

The effects of too little or excessive security staff turnover suggests that there is a “middle of the road goal of controlled turnover.” The management of each healthcare security program is somewhat unique, with dozens, if not hundreds, of variable considerations and factors to be blended into formulating a “controlled turnover” plan. To be sure, organization administrative management, including Department of Human Resources dictums, labor union interactions, community employment levels, and regulatory agencies at all levels are just a few of the challenges for the development and implementation of the “controlled turnover” plan that, once completed, will continue to be an ever-evolving management challenge.
Seven steps for starting and building an effective hospital security K9 program

Mike Angeline HEM, CHSP, CHCM, CAM

K9 programs have been serving a number of hospitals nationally for the past 30 years to improve staff protection, package or contraband detection, and visitor and patient socialization. In this article, the author provides guidance for security directors who may be considering such a program and reviews the elements of the process undertaken by his healthcare system to successfully achieve a K9 capability.

When I first was asked by my CEO what I thought about using K9 in our hospital security program my first thought was, “it is not the place for it”. However, when he brought it up on a second occasion, I thought it was time to investigate the concept further. I conducted a search of hospital security K9 programs and realized that one of our sister hospitals in Michigan had such a program and had been successful in their implementation and operations since 2003.

I reached out to the supervisor of the K9 Security program at the Michigan hospital and arranged for a site visit. Subsequently the road trip from Ohio to Michigan consisted of a security operations manager and supervisor and myself. Frankly, I was skeptical as we met with the Michigan hospital K9 supervisor and he took the time to explain the program and its successes. We basically reviewed the pros and the cons and
from his perspective and the pros outweighed the cons. After our site visit we analyzed what we had learned and eventually formed a proposal that was addressed to the CEO and senior leadership here at Mount Carmel Health. This process started for us in early 2013 and now, in 2015, we have three full-time K9s and were just approved for a fourth. Here is what, I believe, you need to know to start and build an effective K9 program in seven steps:

First - Do Your Homework. Take the time to investigate the pros/cons/risks and benefits. This may include a site visit to another K9 location for learning purposes, extensive contacts for details, internet searches and partnerships. It is simply not enough to go ahead based on one success story. You want to research others and remember that there may be some healthcare cultural differences. For example, the hospital in Michigan provides community support with their K9s. We, however, would not be as involved as extensively in community support, because being located in Columbus, the state capital, we have several K9 agencies. We do support the community with healthcare, safety or security related events from time to time.

Second - Look for Financing. One approach may be fundraising for K9s and another would be to go to your organization's Foundation and make your case. That is precisely what we did. You can also work something out with prospective security officers to see if they are willing to purchase the dog and the hospital essentially leases the services or forms a payback allotment. I have also had inquiries regarding security officers who had K9s in police departments, but have left the department and want their dogs to continue working as a service-working dog, which is what they were bred for. Once you figure out the major costs and how you are going to pay for them, then consider the operations/maintenance costs (this is where homework from step one comes in). You have your concept. You have the risks and benefits. You have the costs.

Third - Present A Written Proposal. It is always best to run the proposal by your VP or the person you report to so he or she is not caught off guard. Once this
is accepted, then provide the written proposal to senior leadership. I recommend that there is not too much detail placed in your proposal and understand your audience. Do not use police jargon or codes in your explanation. You want to focus on SAFETY and the successes shared by others. You want to show that the benefits outweigh the costs and essentially there is an expected return on investment. The largest returns are from:

- Safety or perception of a safer workplace by providing K9s in patrols
- Suspicious package or contraband detection
- Employee engagement
- Pet therapy; socialization with patients
- Visitor engagement/socialization
- Staff protection

The proposal focus would be more on the positive aspects because you have already done your homework and if you did not see the benefits then you shouldn't make the proposal. The senior leadership or legal department may ask the liability questions. Once you get approval, then what?

Fourth - Start the Process. You do not need to re-create the wheel when you have an organization that is willing to share and already has a successful program in place. You may need to make adjustment or add and take some spokes in that wheel. You have to do the following, but not necessarily in this order, as this should be a team approach and you can assign this out.

- Establish a timeline, build your strategy
- Get the entire cost that you are submitting for Foundation funding (or otherwise). This would at a minimum be cost of the dog and the handler training. Part of your homework is to find an appropriate K9 Training program.
- Enter K9 maintenance projected costs in your operations budget (food, supplies, vet, etc.)
- Build a K9 handler job description and run through Compensation to determine fair wages. This would include a Garcia wage for a handler maintaining the dog while at home.
• Get with Legal in developing at least a five year K9 handler agreement with non-compete clause for organization or Foundation gifted dogs. You need to make sure the organization is protected and the agreement fairly covers the employee if an unfortunate event of incapacitation of handler or dog by no fault of their own.

• Develop K9 Security policy/procedures. This may cover keeping the K9 officer safe, grooming, handling in closed spaces, leash control and car travel.

• Select handler interview candidates and have them also interview with the trainer(s) at the K9 training facility so appropriate screening can occur and the prospect understands what will be required. The master trainer should have input.

• Make a handler selection. Go over agreement, JDs, policy, etc.

• Work with Communications Department in communicating the program and perhaps engage employees by instituting a K9 "Naming Campaign." – It is BEST for the handler to supply about five names to choose from as the dog will become part of his or her immediate family when not at work.

• Other logistics; P card or Debit card charged to operating budgets that a K9 handler will use to make K9 related purchases, hotel stays if out of the area training, vet bills, travel costs, pet food, etc. Dietary and vet needs will passed onto the handler by the master K9 trainer.

• K9 vehicle. It is important that the dog has SAFE transport to and from home and work. It is recommended that you propose the costs to the fundraising entity or Foundation or you consider capital unless it meets operation budget guidelines. You can find police cars that have been retired and invest some money into them (paint, body work, engine repair). Get with your Marketing Department as to logos/branding. K9 cages if not already equipped, can be purchased for just about any vehicle and inserted. We allow our
vehicles to be used for home to work transport, training travel and organization supported community events. Any other time, the dog is part of the handler's family and personal automobiles would be used.

**Fifth - Dog is Selected and Training Starts.** The training takes about three months. The dogs go home with the handlers and focus on training should be socialization, patrol, bomb detection, contraband detection and managing aggression. You want to keep all paperwork after the training is complete and the dog is deployed. The paperwork may include vet records, training records, certifications, etc. Remember, you also need enough room for a crate to be kept in the Security office when the dog is not on patrol.

**Sixth - Establish a Metric (monitoring the program).** There needs to be documentation anytime the dog(s) responds to a call. The mere presence of a dog can de-escalate a potentially violent situation. Metrics would include: using K9s for contraband or bomb detection (suspicious package) and special requests for pet therapy. Think about this. If your dog finds illegal substances in a patient's room and these drugs were confiscated, you may have reduced the potential of harm to that patient as he/she would be getting treated with hospital medications.

**Seventh - Provide Leadership Updates as to the Successes of the Program.** Also you will need to ensure community benefits are entered. Recognizing your Foundation's part is important. You will surely get some good exposure from the program and the Foundation or other fund raising should be recognized. Consider K9 trading cards with the Dog info on the card, with the Foundation mentioned. Your organization's social media is another route.

Finally, as indicated, it is so important that you get the K9 Training Facility involved in your selection. Even if your dog was already trained and was part of a previous program, you want your trainer to evaluate the temperament of the dog. We use a trainer that worked in hospitals and understands the challenges of that environment and will check dog candidates before we are even i-
volved in the final selection. If they are not right for hospitals, our trainer will not advance them to us for review. On another note, this is not a magic pill. You should see a decline in emerging aggression when responding to a call with the dog, but sometimes combatants will not calm down or show any reaction, but the mere presence of the dog will make others comfortable (staff, patients, visitors) in a disruptive environment, which is another key factor.

I realize that not every detail could be relayed in this article. Please feel free to contact the author, Mike Angeline, Mount Carmel Health System, Columbus, Ohio if you have any questions at mangeline@mchs.com.