journal of healthcare
PROTECTION management
Volume 36, Number 2

COVID-19 Special Report

Disaster planning: Training for the perils of weapons of mass exposure, 2020
Anthony J. Luizzo, PhD, CFE, CST, (Ret. NYPD), and Bernard J. Scaglione, CPP, CHPA, CHSP

COVID-19's lasting effects on security practices
Lauris V. Freidenfelds

Strategies for the future: Security lessons from COVID-19
James R. Sawyer, CHS-Diplomate, CPP, CHPA

Coping with a pandemic: Practical questions answered
Paul Allena; George Economas, MS; Anthony J. Luizzo, PhD, CFE, CST, (Ret. NYPD); Paul Sarnese, CHPA, CAPM, MSE, MAS; Bernard J. Scaglione, CPP, CHPA, CHSP; Lisa Terry, CHPA, CPP; and Bryan Warren, MBA, CHPA, CPO-1

Be ready for a ransomware attack
Patrick Maloney, CHSS, BS

Cannabis legalization: Issues to consider
Tim Sutton, CHPA, CPP

Ensuring patient and staff safety in non-behavioral health environments
Brendan Riley, MS, CHPA

The ins and outs of metal detection for preventing violence
Bryan Warren, MBA, CHPA, CPO-1

The case for bedside violence risk assessment tools
Charles Hodges, MA

Surveys of workplace violence perceptions, prevention strategies, and prevalence of weapons in healthcare facilities
James D. Blando, PhD; Marilyn Lou Ridenour, BSN, MBA, MPH, CPH, CIC; and Daniel Hartley, EdD

Nightmare in Nova Scotia
Tom Taggart, CHPA

Fire on the mountain: When a massive wildfire meant evacuation of a 140-bed facility
Dave McGraw

The flip side of evacuation: Handling a sudden influx of long-term care patients
Nikki Schilling, NHA, CNA

Facing an emergency? Your Healthcare Coalition can help
Dave Carney, BS, MEP

How an Alabama hospital handled mass casualties from powerful tornadoes
Randy Causey, CHEP

Drones for hospital safety
Peter Ochinko

Collaborating with the police in drug-diversion investigations
John J. Burke

Publication of the International Association for Healthcare Security & Safety

Leading Excellence in Healthcare Security, Safety and Emergency Management

IAHSS
International Association for Healthcare Security & Safety

Disaster planning: Training for the perils of weapons of mass exposure, 2020

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

The COVID-19 pandemic has underscored the need to revisit plans for coping with outbreaks of deadly infectious agents, whether they arise naturally or through a bioterror attack. Here is a roadmap.

(Anthony J. Luizzo, PhD, CFE, CST, (Ret. NYPD), is on the board of advisors of Vault Verify, LLC. He is the former Director of Security Programming for the NYC Mayor's Office of Economic Development and Business Services, former Corporate Director of Security/Loss Prevention for the NYC Health and Hospitals Corporation, President Emeritus of the NY Chapter of the Association of Certified Fraud Examiners, past President of the Society of Professional Investigators, and former editorial advisory board member for Reuters/WG&L/RIA Group – Thomson Publications. Luizzo is an IAHSS member and a frequent contributor to this journal.)

(Bernard J. [Ben] Scaglione, CPP, CHPA, CHSP, is Senior Consultant directing healthcare security services at DVS Security Solutions/Ross & Baruzini. He has a master's from Rutgers University School of Criminal Justice and has served as a security director for more than 25 years in NYC-area hospitals and in multiple capacities for IAHSS, including on the Board of Directors. He is past Chairman of the ASIS International Healthcare Council and past President of the NYC Metropolitan Healthcare Safety and Security Directors Association and has taught as adjunct faculty at Pratt Institute, Interboro Institute, New Jersey City University, and John Jay College Peace Officer Academy. He writes frequently for this journal.)

In response to the COVID-19 pandemic, we offer our third article for this journal on handling emergency situations involving mass exposure contaminates [1] [2]. One of us (Scaglione) has also authored a book speaking to proactive event prevention and effective resolution [3]. In the pages that follow, we provide an Emergency Preparedness Readiness Checklist that can serve as a roadmap for security executives to follow for more effective disaster management, and we expand on the checklist. We offer guidance on protecting hospital staff, patients, and visitors from becoming contaminated, and we address risk assessment engineering and design, proactive risk exposure mitigation, and innovative recovery strategies for mov-

ing forward once emergencies have passed.

ASSESSING RISKS ASSOCIATED WITH EMERGENT RESPONSES

Knowledgeable security executives instinctively understand that well-structured protection assessments help to deepen and strengthen security response planning strategies. Using lessons learned from actual and planned events along with best practices and awareness of current trends helps to make the plan more efficient and effective. Among the critical functions that a comprehensive assessment includes are analyses of entry points; security staffing levels; traffic management; physical security systems; policies and procedures; visitor control; media relations; mass notification; and law enforcement support. A complete and thorough assessment always helps to put facility security on solid ground and on the positive side of the protection curve.

Beyond carrying out in-house initiatives, you can obtain valuable information on current trends and response practices from government agencies such as The Joint Commission, DNV, Homeland Security, and the Federal Emergency Management Agency (FEMA). When assessing risks and response protocols, FEMA breaks down protocols into four phases: mitigation, preparedness, response, and recovery. Although a healthcare facility's response to an emergent event begins after an incident has occurred, response activities should unfold according to a preplanned progression determined in the mitigation-planning phase. The response process embodies recognition that a disaster is occurring, expeditious reporting of the disaster to key personnel, activating the emergency operations plan, launching the Incident Command Center, notifying and mobilizing all hospital personnel, and ensuring that all emergency units remain mobilized until the disaster is officially declared over.

MITIGATION PHASE

Security executives should always try to turn a bright RED light into a GREEN light and get in front of oncoming catastrophes before they are allowed to escalate. One excellent approach is to formulate effective mitigation protocols to lower risk exposure. Mitigation involves pro-

actively identifying potential hazards before they rear their ugly head. It is the most important part of any emergency preparedness process.

With respect to emergency management planning, all hospitals are required to have an effective emergency management plan that adheres to all local, state, and federal laws and meets accreditation standards set by TJC, DNV, CMS or the NFPA. Risk mitigation requires using an assessment tool that can do the job effectively. Many hospitals use the Kaiser HVA as their general assessment tool. To further deepen and strengthen risk mitigation efforts, healthcare institutions can also seek external expertise.

Formulating a security response program

Common components of a security response initiative include:

- mobilizing and managing security department personnel
- target hardening of the facility
- protecting all utilities
- mass notification of personnel
- collaborating with community resources
- preparing for a patient surge
- ensuring regulatory compliance
- monitoring expenses and finances

A main responsibility of the security department is traffic control and implementing institution lockdown requisites during emergencies. Programmatic issues include:

- vehicle restriction and screening
- facility access control
- visitor and patient screening
- building/entry closures
- media and family relations
- emergency department lockdown
- Incident Command Center activation
- hot and cold zone security
- mass notification

PREPAREDNESS PHASE

The preparedness phase focuses on improving response to and recovery from actual events. The most important activity in this phase is the development of

an Emergency Operations Plan (EOP). This plan should be tested on a regular basis so that security personnel are familiar with it and their role in carrying it out. Periodic testing of the plan is strongly advised and should be a facility-wide exercise. Over and above periodic testing, security personnel should continuously receive hands-on training reinforcing their critical first responder role in handling crisis management issues. Training should be continuous so that security personnel know their roles when the emergency response plan is activated. A good rule of thumb is to have emergency response training conducted at annual in-service education initiatives, at in-house planned exercises, and intermittently at roll calls.

Depending on security's role, additional specialized training may also be needed. Training curricula might include:

- hazardous materials identification
- PPE use
- Decontamination and treatment processes
- FEMA Incident Command training
- Use of thermal or other nontraditional devices

RESPONSE PHASE

The response phase is designed to control the negative effects of an emergent situation or event. The main goal in this phase is to help minimize the impact of the hazardous event on facility staff, patients, and operations. Security's central role during a catastrophic event typically includes managing vehicle and pedestrian movement, ensuring that critical notifications are delivered, and implementing institution lockdown.

Controlling Persons and Vehicles

Security is primarily responsible for controlling vehicle and pedestrian access into and out of the hospital buildings and emergency and incident areas. Controlling access may include:

- screening vehicles entering hospital property
- keeping access roads to the emergency department open for ambulance access
- segregating and controlling access for employees, patients, and visitors

Hospital Lockdown

In an emergent event, the hospital may need to lockdown the institution to reduce the potential for unauthorized access into the facility from potentially exposed persons, family members, and the media. All buildings need to be secured and access to the facility limited to essential staff, patients, and some visitors. This process may include:

- locking all entrance doors not in use
- assigning additional staff to each entry point to ensure order and to limit and control access
- closing all ancillary buildings and services
- designating an area for media and family members
- facilitating institution lockdown procedures

Other security department duties may include:

- activation of a mass notification system to alert all hospital personnel
- inauguration of a Hospital Command Center (HCC)
- institution of a transportation program to pick up off-duty employees
- creation of an emergency "hot and cold" access control procedure
- mandating that staff wear masks, related PPE, and full Tyvek suits
- establishing liaisons with community groups, law enforcement, fire, emergency management, and other first responders
- facilitating the transport of the deceased and releasing the deceased to authorized individuals
- safeguarding of law enforcement and VIP property
- enacting patient transport regulations
- organizing an effective supply chain security routing procedure
- instituting appropriate lockdown-related access control technologies
- expediting access for family members of critically ill patients

RECOVERY PHASE

The recovery phase begins in

tandem with the response phase. It involves demobilizing staff and supplies once the disaster is over and also starting the recovery process by going back to normal operations and recording all financial information pertaining to the disaster and the hospital's response. For many healthcare facilities, returning to normal operations as quickly as possibly is essential for financial survival. Plans should describe procedures for re-establishing normal operations following an emergency and include the identities of all of the people involved in the recovery effort. Most important, FEMA should always be contacted for the expertise, resources, and assistance it can provide. As Walt Disney has been quoted as saying, "the way to get started is to quit talking and begin doing." In other words, the more prepared an organization is, the easier the road back to normalcy becomes. Many healthcare facilities underestimate the resources and time necessary to recover adequately from an emergency. Recovery operations should include provisions for staff, facilities, finances, and community support. A detailed recovery plan should include recuperation strategies that do not interrupt normal hospital operations and that help to restore business operations as soon as physically possible.

A well-founded recovery plan should:

- minimize the economic impact of the interruption
- establish alternative means of operation
- train personnel on recovery procedures
- provide for a smooth and rapid restoration
- offer staff support

Recovery planning begins with conducting a risk analysis evaluation report to help identify the most effective method of resuming normal business operations. The analysis should be prepared by competent teams who have business resumption expertise. To help support this evaluation, the following in-house or third-party resources should be made available:

- additional security officers or support personnel
- temporary off-site office facilities
- appropriate technological support (computers, peripherals, communication

equipment, software, and data)
- vital record availability (electronic and hard copy)
- service support (power, natural gas, water, sewer, telephone, internet, wireless)
- security-related systems
- specialized training
- third-party service contracting

A wise individual once said that there is a unique balance between risk and reward. When developing a comprehensive recovery strategy, it is important to focus all recovery efforts so that they snugly fit the specific needs of the particular hospital or healthcare organization under scrutiny. Choosing the right person or people to lead the recovery is one of the first steps in developing an effective plan.

Additional steps to consider when piecing together a plan might include:

- ascertaining federal and local government reimbursement vehicles
- developing a list of vendors, contact information, and supplies
- locating backup facilities
- formulating an operational recovery process
- identifying security technology requirements
- establishing equipment needs

Testing the plan

It is important to always remember that proper planning prevents poor performance. Once a recovery plan is finalized, it is time to vigorously test the system. Unfortunately, all too often organizations do not test the recovery plan or train staff in the recovery process. This part of emergent event response is most important. It can mean the difference between financial stability and bankruptcy.

CONCLUSION

Enlightened security administrators know that the camera of scrutiny will stop at their desk if their institution is *not* ready when disaster strikes. Hospitals and long-term care institutions should never be inactive in the face of need. Regardless of whether a disaster is a pandemic event, a terrorist attack, an active assailant offense, a workplace violence incident, or a

weather event, the institution must to be ready to tackle the catastrophe. The key to staying one step ahead of failure is to continually evaluate existing emergency response plans and implement appropriate training to help keep hospital staff current and ready for future onslaughts.

Recovery plans need to be reviewed and tested on a regular basis and programmatic enhancements enacted when necessary. It is important that every security executive understand that quick and innovative security action helps to determine the security department's destiny.

References

1. Luizzo, A., & Scaglione B. (2007). Training security officers to recognize the perils of weapons of mass destruction and pandemic flu contaminates. *Journal of Healthcare Protection Management*, *23*(2), 1–9.

2. Luizzo, A., & Scaglione B. (2019). Training security officers to recognize the perils of weapons of mass exposure contaminates – part II. *Journal of Healthcare Protection Management*, *35*(1), 32–39.

3. Scaglione, B. (2019). *Security management for healthcare: proactive event prevention and effective resolution.* New York, NY: Routledge/Productivity Press.

Emergency Preparedness Readiness Checklist

Review each item, and check one box Yes, No, or N/A (not applicable). If No is checked for any item, explain in the comment box.

Section 1: Risk Assessment	Yes	No	N/A
1. Has an annual risk assessment been prepared?	❑	❑	❑
2. Does the risk assessment include all phases of the emergency preparedness plan?	❑	❑	❑
3. Does the risk assessment Include all training updates?	❑	❑	❑
4. Does the risk assessment Include drill evaluation compliance?	❑	❑	❑
5. Does the risk assessment Include actual event evaluation compliance?	❑	❑	❑
6. Does the risk assessment meet regulatory compliance standards?	❑	❑	❑
Additional Comments:			

Section 2: Mitigation Phase	Yes	No	N/A
1. Is an emergency management plan available?	❑	❑	❑
2. Are potential hazards identified?	❑	❑	❑
3. Does the plan meet regulatory compliance requisites?	❑	❑	❑
4. Does the plan properly address mobilization strategies?	❑	❑	❑
5. Are target hardening recommendations adequate?	❑	❑	❑
6. Are utility security concerns addressed?	❑	❑	❑
7. Does the plan adequately address personnel and other notification essentials?	❑	❑	❑
8. Are community resources included?	❑	❑	❑
9. Have fiduciary issues been addressed?	❑	❑	❑
10. Are access control strategies included?	❑	❑	❑
11. Have media and family relations issues been addressed?	❑	❑	❑
12. Other issues:	❑	❑	❑
13. Other issues:	❑	❑	❑
Additional Comments:			

Section 3: Preparedness Phase	Yes	No	N/A
1. Does the plan include an Emergency Operations Plan (EOP)?	❑	❑	❑
2. Has the plan been periodically tested?	❑	❑	❑
3. Have tests been properly evaluated and corrective measures implemented?	❑	❑	❑
Additional Comments:			

Section 4: Response Phase	Yes	No	N/A
1. Does the plan adequately control pedestrian and vehicular movement?	❑	❑	❑
2. Does the plan address emergency vehicle access?	❑	❑	❑
3. Does the plan designate employee, patient, and visitor access particulars?	❑	❑	❑
4. Does the plan adequately address institutional lockdown measures?	❑	❑	❑
5. Does the plan include beefed-up staffing at strategic access points?	❑	❑	❑
6. Does the plan address ancillary building and service closures?	❑	❑	❑
7. Does the plan earmark media and family member billets?	❑	❑	❑
8. Does the plan define institution lockdown maneuvers?	❑	❑	❑
Additional Comments:			

Section 5: Recovery Phase	Yes	No	N/A
1. Is a recovery plan available?	❑	❑	❑
2. Does the recovery plan spell out when the institution can return to normal operations?	❑	❑	❑
3. Does the plan contain disaster-related fiduciary documentation?	❑	❑	❑
4. Does the plan contain economic impact interruption data?	❑	❑	❑
5. Does the plan contain alternative institutional operational models?	❑	❑	❑
6. Is the staff adequately trained to handle recovery procedures?	❑	❑	❑
7. Does the plan address restoration prerequisites?	❑	❑	❑
8. Does the plan offer staff support?	❑	❑	❑
Additional Comments:			