SAFETY AND SECURITY CONSIDERATIONS FOR HOSPITALS

555 WEST 57TH STREET, NEW YORK, NY 10019 • T (212) 246-7100 • F (212) 262-6350 • WWW.GNYHA.ORG • PRESIDENT, KENNETH E. RASKE

Hospitals face unique challenges related to safety and security. First and foremost, they strive to provide a compassionate, accessible, and inviting environment where patients, visitors, and staff can move with relative freedom as they receive care, visit loved ones, and deliver care throughout large and complex institutions. As an example, a hospital outpatient might need to travel to multiple locations in several hospital buildings in one day, visiting first a physician, then an imaging center, then perhaps a laboratory.

At the same time, hospitals are expected to provide a safe environment, and to anticipate the possibility of unstable or impaired patients, conflicts between patients and family, disgruntled current or former employees, and security threats from the surrounding community.

GNYHA WORKGROUP

To help members address the safety and security challenges hospitals face, Greater New York Hospital Association (GNYHA) convened a workgroup of health care security directors and external law enforcement representatives. As part of its efforts, the workgroup reviewed a previously developed GNYHA document on hospital security to update it in light of the current environment.

OVERRIDING THEMES AND GUIDANCE

An overriding theme that emerged in workgroup meetings was the importance of establishing a culture of security by involving and empowering facility employees, visitors, and vendors, as well as implementing a layered security approach that accounts for the unique vulnerabilities of certain hospital areas.

The workgroup also identified two organizational or foundational steps hospitals can take to improve their culture of security. First, as with other preparedness activities, an organization should consider *undertaking a vulnerability analysis of its operations oriented toward safety and security concerns*. For this process, the workgroup recommended paying particular attention to vulnerable locations such as research labs, psychiatric areas, and the Emergency Department.

Next, the workgroup recommended *developing a mechanism for reporting and tracking security incidents*, including thefts, threats with and without weapons, and physical altercations. For this purpose, the workgroup recommended that all incidents, whether they involve employees, patients, visitors, or any combina-

tion thereof be reported and tracked. Routine analyses of incident reports can inform assignment of security resources, targeting of training, and identification of areas where additional security measures are most needed. It can also inform workflow and protocol changes. For example, one hospital identified that patients arriving for blood work often became agitated due to long wait times. In response, the hospital improved its communications with those patients when scheduling appointments. Upon arrival, the patients anticipated the waiting involved, resulting in less distress.

SPECIFIC CONSIDERATIONS AND STRATEGIES

The workgroup also identified key areas for hospitals to review as they consider improving their approach to safety and security. GNYHA organized these considerations into four sections, providing a fifth section that contains tools and resources. Although we do not include a specific section on active shooter or armed intruder situations, many of the security considerations in this document can serve as deterrents to such incidents. We also include several active shooter tools in the Resources section.

GNYHA emphasizes that the security standards and regulations promulgated by the Centers for Medicaid & Medicare Services, The Joint Commission, and the New York State Department of Health or other state requirements should serve as the foundation for a security program. GNYHA thus offers the considerations in this document to complement and further strengthen facilities' actions to meet and maintain compliance with those standards.

GNYHA also emphasizes that the considerations should not be viewed as setting a standard for security. Rather, they should serve as a vehicle to help members review security measures within the context of their own operations, ideally by means of inter-disciplinary conversations among security, human resources, emergency management, and clinical leadership. Finally, we note that some considerations might relate to more than one topic and may appear in several separate sections.

If you have questions or need assistance with these or related resources, please contact Patrick Meyers (pmeyers@gnyha.org or 212-258-5336) or Jenna Mandel-Ricci (jmandelricci@gnyha.org or 212-258-5314).

Staff and Vendor Management

Comprehensive staff and vendor management policies are an important component of a secure facility. This section offers numerous practices for consideration when hiring, onboarding, and training new employees and vendors. Other areas outlined are the identification and screening of vendors, and the security of staff who work in community settings such as home visiting programs. For the purposes of this document, contractors and vendors working in a facility for more than two consecutive days, or for a specified contract term, should be treated the same as those employed by the facility.

HIRING & ONBOARDING

HIRING

- Conduct background checks on employees and vendors. When reviewing the results, involve appropriate staff from security, legal, and risk management to make informed hiring decisions.
- When reviewing a prospective employee's/vendor's background, if they have a criminal history, consider the length of time since the conviction and the pertinence of the conviction to the prospective role.
  - **Special note**: Some states, including New York State, have laws stipulating when and how criminal background check information may be used in hiring and employment decisions. Consult your legal and risk management departments to ensure compliance with employment regulations.

ONBOARDING

- Provide all new employees with a copy of the facility's security policies and procedures, and have employees acknowledge receipt.
- Train all new vendors and contractors on facility security policies and procedures, and have them acknowledge receipt of the training and security policies.

TRAINING & EDUCATION

- Provide security training as part of new employee orientation. Annual refresher training, including on safety and security measures, for all employees is also recommended.
- Train all staff on what is a reportable incident, how to report incidents, and expectations for incident reporting. Train employees and vendors to recognize and appropriately report "suspicious behavior" to security.
- If the facility has employee only entrances (see *Physical Security* section), train employees and vendors on security protocols and expectations related to the entrances.
- Consider offering de-escalation training to all employees, or employees in areas of the hospital where conflict or agitation has been previously reported.
- Encourage staff with *Orders of Protection* to share information with security staff and develop a work safety plan.

IDENTIFICATION

- Develop and implement clear policies about the wearing of hospital identification (ID) by employees and vendors.
  - If an employee or vendor does not have an ID, he/she should be verified as an employee/vendor, then issued a temporary ID.
  - Employees and vendors should be instructed to report lost or stolen IDs to hospital security. Human resources and security should work together to track such incidents.
  - The hospital should develop and communicate policies for employees/vendors who report to work without their ID.
- Consider the use of oversized identification cards, with symbols or colors indicating access to specific areas of the hospital.
- Consider the use of authentication measures on all IDs such as holograms.
- Consider setting routine expiration dates on IDs.
  - For temporary staff or vendors, consider pre-setting expiration dates on IDs tied to the anticipated contract period or period of employment. This same procedure can be used for non-hospital/non-network clinical staff who may be provided a temporary ID during an emergency situation.
- If the hospital uses electronic access control systems, link them whenever possible to staff management systems to deny access upon termination of employment.
- Consider using employee only entrances that require staff to show ID or require key card swipe for entry.

EMPLOYEE TERMINATION

- Involve both human resources and security in the development and implementation of all termination policies and procedures.
- When delivering a notice of termination to an employee, document any threatening comments or unusual behavior.
- Involve two or more individuals in any employee termination conversation.
- Law enforcement experts recommend terminating employees on a Friday, providing a built-in "cooling off" period.
- Inform security staff and staff of an employee's assigned unit(s) of an employee's termination.
- Take possession of all hospital identification upon termination of an employee, along with any access cards, keys, and identifying uniform or clothing. Some facilities pair the release of the terminated employee's last paycheck with the return of hospital property. The same rule should apply to vendors who are terminated or whose contract period has ended.

SECURITY CONSIDERATIONS FOR STAFF IN COMMUNITY OR HOME SETTINGS

- Encourage staff to travel in pairs when possible.
- Consider providing panic alarms or providing smartphone applications with such features for staff working in community settings.
- Consider implementing check-in procedures. If staff members fail to check in at the assigned time, security staff can proactively reach out to the employee.

Patient and Visitor Management

Managing the presence of patients and visitors is an important security feature. This section describes several strategies and considerations including visitor management systems, patient and visitor education, visitor access, and available technology.

VISITOR ENTRY, EDUCATION, AND DE-ESCALATION

- Assign staff at entry points so individuals entering a facility have contact with security personnel or other facility representatives. Consider having visitors sign a logbook upon entering and exiting, or be processed through a visitor management system and given identification to wear while in the facility.
- Consider making available safety and security information to patients and visitors. This could include a palm card or small brochure with: a map of the facility, evacuation information, what to expect during an emergency, or how to identify and report suspicious behavior. This information could also be shared via electronic means—e.g., patient televisions, guest internet landing page.
- Identify areas and departments where patients and visitors commonly become upset. In these areas:
  - Consider workflow changes and messaging to address common sources of agitation.
  - Offer de-escalation training to employees.
  - Develop protocols to quickly surge specially trained staff (e.g., security staff, social workers) to offer assistance.

IDENTIFICATION

- Consider adopting a visitor management system.
  - Encourage visitors to wear identification at all times.
  - If it is a feature of the selected visitor management system, indicate the visitor's destination (e.g., unit, department) on the identification.
- Train staff to use the provided visitor identification to verify that an individual should be present on a particular unit. If the visitor's ID indicates another location, staff should be trained to redirect the individual.
- Consider additional visitor access control equipment for sensitive areas of the hospital.

TECHNOLOGY

- Consider use of visitor management software systems that produce temporary identification for visitors. If purchasing such a system, consider the following capabilities:
  - Ability to print a photo of the visitor on the temporary identification.
  - Ability to include visitor destination information on the temporary identification.
  - Ability to scan an individual's driver's license and compare it to external databases.
- Consider integration of facial recognition software that may be helpful in high-risk areas such as research labs, or in alerting security staff to high-risk visitors such as terminated employees who have made threats.
- Consider adding magnetometers (i.e., metal detectors) to help prevent the entry of concealed weapons or prohibited items into the facility. Handheld and stand-up magnetometers can be a component of a facility physical security plan.

Physical Security

This section outlines a variety of considerations to improve physical security, including training and educating staff, vendors, patients, and visitors; suggested identification processes; infrastructure and technology considerations; and incident specific response kits. As noted earlier, many of the considerations found in this section are also reflected in other sections of this document.

TRAINING & EDUCATION

STAFF AND VENDORS

- Provide security training as part of new employee orientation. Annual refresher training for all employees regarding safety and security measures is also recommended.
- Train all staff on what is a reportable incident, how to report incidents, and expectations around incident reporting. Train employees and vendors to recognize and appropriately report "suspicious behavior" to security.
- If the facility has employee only entrances, train employees and vendors on security protocols and expectations related to these entrances.
- Consider offering de-escalation training to all employees, or employees in areas of the hospital where conflict or agitation has been previously reported.
- Encourage staff with *Orders of Protection* to share information with security staff, and develop a work safety plan.

PATIENTS AND VISITORS

- Consider making available safety and security information to patients and visitors. This could include a palm card or small brochure with: a map of the facility, evacuation information, what to expect during an emergency, or how to identify and report suspicious behavior. This information could also be shared via electronic means – e.g., patient televisions, guest internet landing page.

IDENTIFICATION

STAFF AND VENDORS

- Develop and apply clear policies related to the wearing of hospital identification (ID) by employees and vendors.
  - If an employee or vendor does not have an ID, he/she should be verified as an employee/vendor, and then issued a temporary ID.
  - Employees and vendors should be instructed to report lost or stolen IDs to Hospital Security. Human Resources and Security should work together to track such incidents.
  - The hospital should develop and communicate policies for employees/vendors who report to work without their ID.
- Consider the use of oversized identification cards, with symbols or colors that indicate access to specific areas of the hospital.
- Consider the use of authentication measures on all IDs, such as holograms.

- Consider setting routine expiration dates on IDs.
- If the hospital uses electronic access control systems, link these systems whenever possible to staff management systems to deny access upon termination of employment.
- Take possession of all hospital identification upon termination of an employee or vendor, along with any access cards, keys, and identifying uniform or clothing. Some facilities choose to pair the release the terminated employee's last paycheck with the return of hospital property.
- Consider use of employee only entrances that require staff to show ID or require key card swipe or entry.

VISITORS

- Consider adoption of a visitor management system.
  - Encourage visitors to wear identification at all times.
  - If a feature of the selected visitor management system, indicate the visitor's destination (e.g., unit, department) on the identification.
- Train staff to use the provided visitor identification to verify that an individual should be present on a particular unit. If the visitor's ID indicates another location, staff should be trained to redirect the individual.
- Consider additional visitor access control equipment for sensitive areas of the hospital.

SECURITY PERSONNEL

- Consider the use of a law enforcement paid detail program to augment your security staff in particular areas or during particular shifts. Contact your local law enforcement agencies to inquire about having a paid police presence in or around your facility.

TECHNOLOGY

SECURITY CAMERAS

- Consider use of fixed cameras to monitor and record activity in specific locations, and movable cameras for assessing situations.
- Prioritize placement of cameras at pedestrian entrance/exits, and high traffic internal public spaces.
- Record and maintain footage for no less than 60 days, ensuring images are of high enough resolution to identify people and objects.
- Consider magnetometers (i.e., metal detectors) to aid in preventing the entry of concealed weapons or prohibited items into the facility. Hand-held and stand-up magnetometers can be a component of a facility physical security plan.
- Consider providing personal panic buttons (worn on person) to staff in sensitive areas such as in the Emergency Department and behavioral health units.
- Consider placing stationary panic buttons in sensitive areas such as pharmacies, research areas, and areas with sensitive equipment (e.g., blood irradiators).
- Develop complementary security protocols tied to panic button use.

RETINA SCANNERS

- Consider use of retina scanners in areas with sensitive equipment and materials including pharmacies, research areas, and the blood bank.

FIRST RESPONDER ACCESS KIT

- Consider creating and maintaining an access kit to improve coordination with law enforcement and other first responders during events such as the presence of a high profile patient or an active shooter incident. Kits should include facility blueprints, and all access key and swipe cards, and should be housed in a locked, waterproof case.
- Consider placing kits at each staffed entrance or security station. Protocols related to accountability, security, and updating of procedures contained within the kits should be developed, implemented, and maintained.

SIGNAGE

- Post appropriate signage near all restricted areas with instructions on how to gain access to the area should temporary access be required. Messages may include:
  - "Unauthorized Personnel Not Permitted. To gain access, please contact Security."
  - "Authorized Personnel Only. To gain access, please contact Security."
  - "Only visitors with [x] designation are permitted. For assistance, please contact [x]."
  - "Employees Only. Visitors, please use main entrance located [LOCATION]. All others, please contact Security for admittance."

Emergency Department

The most dynamic environment in any facility is the Emergency Department (ED). In addition to managing day-to-day security threats, it is important that facility security directors, ED leadership, and emergency managers work together to formulate a specific plan for high impact events in the ED. This plan might include the ability to surge security staff, having a pre-identified location for law enforcement to set up a centralized command and control area, and the ability to limit egress to the ED. ED staff should be aware of what actions security and law enforcement personnel will take during such events. This ED section contains these and other strategies.

TRAINING & EDUCATION

STAFF AND VENDORS

- Consider making available safety and security information to patients and visitors. This could include a palm card or small brochure with: a map of the facility, evacuation information, what to expect during an emergency, or how to identify and report suspicious behavior. This information could also be shared via electronic means – e.g., patient televisions, guest internet landing page.
- Proactively identify scenarios within the ED where patients and visitors commonly become upset, such as prolonged waits to be seen, or delays while waiting for discharge paperwork.
  - Consider workflow changes and messaging to address common sources of agitation.
  - Offer de-escalation training to all ED staff.
  - Develop protocols to surge specially trained staff with limited notice (e.g., security staff, social workers) to offer assistance.

PATIENT AND VISITOR MANAGEMENT

- Assign staff at entry points so that individuals entering the ED have contact with security personnel or other facility representatives. Visitors should sign a logbook upon entering and exiting, or be processed through a visitor management system and given identification to wear while in the facility.
- Consider limiting the number of visitors at the bedside in the ED. If your facility has such a policy, ensure there is visible signage indicating this policy.

ADDITIONAL CONSIDERATIONS

- Limit access from the ED to other areas of the hospital.
- Maintain a security presence at all ED entrances and exits, including the ambulance bay. Limit access to the ambulance bay to marked emergency vehicles and on-duty first responders (Police, Fire and EMS) on official business. All others should be directed towards the appropriate entrance or exit.
- Formulate, implement, and exercise plans for high-impact events affecting the ED such as mass casualty events and high-profile visitors. Considerations should include surging clinical and security staff, lockdown procedures, media management, and law enforcement coordination.

Tools and Resources

GNYHA RESOURCES

RESOURCE NAME	GNYHA LAW ENFORCEMENT COORDINATION DOCUMENT
Description:	Law enforcement agencies often need to conduct investigations within hospitals in the wake of an emergency, or in advance of high-profile events or dignitary visits. This tool addresses coordination among law enforcement/investigative agencies and hospitals under these and other scenarios. It offers guidance on ongoing hospital communication with local law enforcement, strategies for securing your facility, and recommended actions for specific events.
Link:	https://www.gnyha.org/tool/hospital-coordination-with-law-enforcement-guidance-document/

TRAINING AND ASSESSMENT PROGRAMS

RESOURCE NAME	NEW YORK POLICE DEPARTMENT (NYPD) SHIELD
Description:	SHIELD is an umbrella program for a series of NYPD initiatives that pertain to private sector security and counterterrorism. SHIELD is a public-private partnership designed to provide best practices, lessons learned, counterterrorism training opportunities, and information sharing. SHIELD seeks to partner with private sector security managers with the goal of protecting New York City from terrorist attacks.
Link:	http://www.nypdshield.org

RESOURCE NAME	NATIONAL SHIELD NETWORK
Description:	For areas outside of New York City that wish to launch a SHIELD program, please reach out to NYPD SHIELD to inquire about the National SHIELD Network.
Link:	http://www.nypdshield.org

RESOURCE NAME	US DEPARTMENT OF HOMELAND SECURITY (DHS) CRITICAL INFRASTRUCTURE PROTECTION PROGRAM
Description:	The Office of Infrastructure Protection's Assist Visits are a cornerstone of the agency's voluntary outreach effort to critical infrastructure owners and operators. An Assist Visit, conducted by DHS Protective Security Advisors, is designed to: • Provide a comprehensive assessment of both the security strengths and weaknesses within a facility. • Provide assessment tools to gauge where facilities should make investments and what the potential outcomes of those investments may yield. • Provide an overview of the Office of Infrastructure Protection resources available to the facility to enhance security and resilience. Interested facilities can contact John Durkin, Chief of Protective Security, DHS, Region II, at John.durkin@HQ.dhs.gov or (646) 235-7808.
Link:	https://www.dhs.gov/assist-visits

ACTIVE SHOOTER AND WORKPLACE VIOLENCE RESOURCES

RESOURCE NAME	ACTIVE SHOOTER PLANNING AND RESPONSE IN A HEALTHCARE SETTING (2017, 3RD EDITION)
Description:	Produced by the Healthcare and Public Health Sector Coordinating Council, which is co-led by US DHS and US Health and Human Services, this document draws on the expertise of public and private sector leaders to address the unique challenges of an active shooter event within a health care setting. It includes discussion of vulnerable patients, hazardous materials, and locked units. The document also includes an ethical considerations section.
Link:	https://www.fbi.gov/file-repository/active_shooter_planning_and_response_in_a_healthcare_setting.pdf/view

RESOURCE NAME	OSHA'S GUIDELINES FOR PREVENTING WORKPLACE VIOLENCE FOR HEALTHCARE AND SOCIAL SERVICES WORKERS
Description:	Recognizing the increased risks to healthcare and social service workers, these 2016 violence prevention guidelines are based on industry best practices and feedback from stakeholders. The document includes recommendations for developing policies and procedures to eliminate or reduce workplace violence in a range of healthcare and social service settings.
Link:	https://www.osha.gov/Publications/osha3148.pdf

RESOURCE NAME	AMERICAN ORGANIZATION OF NURSE EXECUTIVES/EMERGENCY NURSES ASSOCIATION TOOLKIT FOR MITIGATING VIOLENCE IN THE WORKPLACE
Description:	Originally disseminated in 2015, this toolkit addresses employee-on-employee, and patient and family violence in the hospital setting.
Link:	http://www.aone.org/resources/mitigating-workplace-violence-Tool%20Kit

RESOURCE NAME	FEDERAL BUREAU OF INVESTIGATION (FBI) ACTIVE SHOOTER RESOURCES
Description:	The FBI provides operational, behaviorally-based threat assessment and threat management services to help detect and prevent acts of targeted violence, helping academic, mental health, business, community, law enforcement, and government entities recognize and disrupt potential active shooters who may be on a trajectory toward violence. Resources include developing and incorporating emergency plans for various institutions, research studies, analyses, trainings, and recovery resources with regards to hostile situations.
Link:	https://www.fbi.gov/about/partnerships/office-of-partner-engagement/active-shooter-resources

RESOURCE NAME	INCORPORATING ACTIVE SHOOTER INCIDENT PLANNING INTO HEALTH CARE FACILITY (HCF) EMERGENCY OPERATIONS PLANS
Description:	This document, jointly developed by US HHS, DOJ, DHS, and FEMA, is designed to assist facilities in preparing for an active shooter incident. Though hospitals and many other HCFs have emergency operations plans, this document provides emergency planners, disaster committees, executive leadership, and others involved in emergency operations planning with detailed discussions of unique issues faced in an HCF. This document also includes discussions on related topics, including information sharing, psychological first aid, and law enforcement/security coordination.
Download Link:	https://www.hsdl.org/?view&did=760849 (PDF will download when clicked)

RESOURCE NAME	THE JOINT COMMISSION WORKPLACE VIOLENCE PREVENTION RESOURCES PORTAL
Description:	The portal links to materials from The Joint Commission, government resources, and professional associations such as the American Nurses Association and the American Hospital Association, and its personal membership groups and related organizations.
Link:	https://www.jointcommission.org/workplace_violence.aspx

RESOURCE NAME	METROPOLITAN HEALTHCARE SECURITY DIRECTORS ASSOCIATION *PLAN TO LIVE* ACTIVE SHOOTER TRAINING VIDEOS
Description:	The Metropolitan Healthcare Security Directors Association (MHSDA) created an active shooter training video series called *Plan to Live*. Module 1 focuses on preparing staff for an active shooter scenario, while Module 2 focuses on leadership and executive staff preparedness. The videos are available to MHSDA members via the Academy portion of the MHSDA website, and can be used for training purposes.
Link:	www.mhsda.org

RESOURCE NAME	US DEPARTMENT OF HOMELAND SECURITY ACTIVE SHOOTER PREPAREDNESS RESOURCES
Description:	A compilation of training resources, materials, and templates to prepare communities for Active Shooter situations. Resources are available for the following audiences: • Private Citizen • Human Resources or Security Professionals • Active Shooter Workshop Participants • First Responders All resources are available in multiple languages.
Link:	https://www.dhs.gov/active-shooter-preparedness

RESOURCE NAME	US DEPARTMENT OF HOMELAND SECURITY BOMB THREAT PREPAREDNESS
Description:	A compilation of trainings, videos, documents and other resources to educate individuals on what do to in the event a suspicious item is found, or a bomb threat is made.
Link:	https://www.dhs.gov/what-to-do-bomb-threat