MHA SECURITY GUIDANCE:

Developing Healthcare Safety & Violence Prevention Programs within Hospitals

MASSACHUSETTS Health & Hospital ASSOCIATION

March 2019

Table of Contents

Introduction

Massachusetts hospitals continue to be committed to the protection, health, and wellbeing of our healthcare workforce and patient populations. This includes developing policies and procedures to prevent threatening or intimidating conduct and actual physical violence within hospitals and healthcare settings.

In response to concerns regarding increased risk of violence in healthcare settings, the Massachusetts Health and Hospital Association (MHA) formed a Workplace Safety and Violence Prevention Workgroup composed of a diverse group of hospital staff including, but not limited to, healthcare security professionals, nursing leadership, and legal counsel. The workgroup developed the following guidance to provide an understanding of the current best practices being used across Massachusetts hospitals with the goal of providing a framework for an effective healthcare violence prevention program. Such a program includes adopting a formal method for staff to report incidents of violence and for hospital management to review and analyze incidents, data, and trends to consider appropriate prevention efforts within and throughout the hospital's properties. Finally, this guidance supports hospital adoption of internal security alert systems within the electronic medical record that will inform clinical staff and security about a patient's previous history and potential risk for violent behavior to assist with proactive in the moment prevention efforts prior-to and during an encounter with said patient.

The workgroup developed the following definition of "healthcare violence" to ensure standardization of how incidents are reported across Massachusetts healthcare settings. This definition of healthcare violence includes actions by patients, other employees, and outside visitors (interpersonal and non-interpersonal) and has been modified from the language used by the CDC National Institute for Occupational Safety and Health and the US Department of Labor.

> Healthcare violence shall include violent acts, including physical assaults, threats of assaults, intimidating conduct, and workplace conflict directed towards persons at work or on duty. Assault within a healthcare facility setting includes two distinct actions, which includes: (1) intentional assaults (verbal, attempted contact, actual physical contact) intending to cause or is capable of causing death or serious bodily injury to self, others, or damage to property; and (2) unintentional assault by a patient or other individual who is not aware of their actions due to a medical condition, medication, or following a medical procedure. Finally, healthcare violence within the healthcare setting also includes intimidating or harassing behavior to hospital staff within the facility or outside of the hospital.

There are legal protections for staff that experience violence in a healthcare setting. Hospitals and healthcare facilities are also required under existing state and federal requirements to develop general policies regarding violence prevention for healthcare workers. These include the following:

- In Massachusetts, Chapter 151 of the Acts of 2010 puts into place enhanced penalties (fines and/or jail time) for an assault or an assault and battery on a healthcare provider while treating or transporting a patient in the line of duty.
- In 2015, the Executive Office of Health and Human Services issued regulations (101 Code of Massachusetts Regulations 19.00), pursuant to state law (Section 30 of Chapter 3 of the Acts of 2013) that requires any program that provides direct services to clients and is operated, licensed, certified or funded by a department or division of the Executive Office of Health and Human Services to have a workplace violence prevention and crisis response plan, updated at least annually, for social workers, human services workers, volunteers, and all other employees. Programs are required to provide a copy of the current plan to any employee of the program upon request.
- The Joint Commission (TJC), as part of the hospital accreditation program and routine survey, requires hospitals to meet various standards regarding the development of workplace violence prevention policies and services. The specific requirements are found within the (1) environment of care, (2) emergency management, and (3) leadership standards, which are incorporated into the Medicare Conditions of Participation and the Department of Public Health hospital licensure regulations. TJC issued these standards in its Sentinel Event Alert (Publication Issue 59, April 17, 2018) that provides an overview of TJC's expectations when a survey is conducted at a hospital.

Healthcare Violence Prevention Efforts within the Hospital

It is recommended that each hospital incorporate healthcare violence prevention program oversight within an already existing committee focused on evaluating safety and operations, or develop a separate broad-based multidisciplinary Workplace Violence Prevention Committee. The goal of the committee is to design, implement, modify and evaluate a healthcare violence prevention program for their facility or organization and to drive system-level improvements for reducing potential violent incidences in a healthcare setting. These efforts should include the entire facility to ensure that prevention programs are effective and accessible to all facility employees, patients, and visitors. This work may consist of, but is not limited to, providing input on the redesign of built environment and facilities, improving policies and procedures, and ensuring there is a comprehensive data reporting and collection process in place for ongoing review and assessments.

Developing an effective and sustainable program to ensure prevention of healthcare violence requires (1) support from senior leadership, (2) broad based collaboration among departments, and (3) commitment to sustain internal improvements and policies.

STEP 1 **Gain Leadership Support**	Hospital senior management should commit to the development and sustainability of this prevention effort by allocating resources for the appropriate committee to conduct internal risk assessment for all locations (on and off-campus) and develop an internal process for proper reporting of incidents for committee review and analysis. Hospital senior management should also ensure there is an appropriate policy publicly posted in all locations that makes clear the organization's position on incidents of violence, including the consequences of committing such acts.
STEP 2 **Collaboration Across the Hospital**	When developing hospital policies and practices, it is critical to include representation from all departments, personnel, and organizations that will help drive internal review and possible changes based on the internal risk assessment. The committee that is directed to manage this issue may include members of front-line staff from departments and units at high risk, staff within employee assistance programs, risk management, with healthcare professionals leading or co-chairing the overall effort. Further, the facility should consider including staff from legal, behavioral health, and other senior clinical and operational staff, where applicable. Finally, the committee should also consider consulting with the hospital's Patient Family Advisory Council (PFAC) for patient engagement.
STEP 3 **Sustainability of Improvement through Dedicated Resources**	The committee overseeing healthcare violence prevention should use internal incident reports to properly assess current operations, determine the need for appropriate safeguards, review specific operational changes, determine what resources are needed, and implement changes in an effort to minimize known areas of risk and violence. The hospital should consider appropriate technology investments that would allow the facility to measure the performance of implemented recommendations in reducing healthcare violence incidents. Finally, an appropriate staff from the committee should present an overview of the internal reports and proposed operational changes needed to the hospital senior management and, as appropriate, to the hospital's governing body.

Risk and Threat Assessment

Each healthcare organization should conduct a routine risk and threat assessment (at a frequency appropriate to your facility) that includes employee engagement or a security survey of all locations covered under a hospital license and compares and analyzes the risk of violent incidents. This assessment may entail gathering data that reflects the "who, what, how, where, when, and why" of a hospital's existing security operations. The goal of this analysis is to identify the types of hazard prevention and control measures that may be needed to avoid incidents of violence. Some components may include:

Records review: Hospitals should determine what information is currently maintained by the facility to assist with reviewing areas or situations of concern. Suggested resources that the hospital should consider include information that is maintained by security leadership, risk management, and employee health/human resources departments. Examples of the information that may be helpful in the analysis includes documented reports of assaults (verbal, attempted, and/or actual physical) that are intentional or unintentional, threat assessments, worker's compensation related to physical/verbal assaults, insurance records, work related injuries and illnesses reports required by OSHA, first reports of injury, incident and near-miss logs, incident reports, police reports, event logs, and other daily logs.

Procedures: An analysis of the site's operations and procedures to identify if they contribute to hazards related to healthcare violence. This includes addressing the relationship between employees, job positions, job specific tasks, position tools and resources, and work environment.

Employee Engagement: Hospitals should engage with employees before and after operational or policy changes in a manner that takes into account the size, structure, and environment of each facility. While some hospitals have conducted routine surveys, depending on their employee size, others have found it effective to engage with their employees through staff meetings and routine hospital rounds. It is important to include participation from employees to identify types of problems workers face and assess effects of changes on their perceived feelings of safety and effectiveness of training. For the employee engagement, suggested questions to consider include the following:

- What daily activities expose you to the greatest risk of violence?
- What work activities make you feel unprepared to respond to a violent incident?
- Can you describe how a change in a patient's daily routine affected the precautious you take to address the potential for healthcare violence?
- Can you recommend any changes or additions to the healthcare violence prevention training that will help you assess and manage possible risks?

Finally, it is critical that hospitals also conduct an employee de-brief following an incident involving not only the employee who was directly affected, but others who were in the department or area when the incident occurred. This ensures that the specific information about the incident and the perspective of the employees are obtained and can be included in any follow-up activities. Any engagement and documented results should be done in coordination with human resources to ensure that engagement and maintenance of employee information follows policies in the applicable employee manual(s) for the facility.

Security Assessment: Walk through assessments focused on high-risk departments and units, including but not limited to psychiatric units, emergency departments, geriatrics, admissions, maternal and child health, and waiting rooms. This analysis should also include external assessment of hospital grounds and building areas, parking, and the evaluation of security measures (i.e. duress and alarm devices).

Patient Feedback: In forming their threat analysis, hospitals should consider the input of patients and families, which can be obtained through patient surveys, focus groups, interviews, and research. Organizations should consider engaging existing patient and employee workgroups (such as the patient family advisory committee (PFAC)).

There are various industry standard tools organizations can use or incorporate into their threat analysis. Some examples include:

- American Society for Healthcare Risk Management Workplace Violence Toolkit: http://www.ashrm.org/resources/workplace_violence/pdfs/Workplace-Violence-Tool.pdf
- ASIS Healthcare Security Council: https://community.asisonline.org/communities/community-home?CommunityKey=7526f103-fee3-41bc-8f4e-00d3c48b0adb
- International Association for Healthcare Security and Safety Guidelines (IAHSS): https://www.iahss.org/page/guidelines
- Public Services Health and Safety Association (PSHSA) Workplace Violence Risk Assessment Toolkit for Acute Care: https://www.pshsa.ca/wp-content/uploads/2017/05/VPRASAEN0417-Workplace-Violence-Risk-Assessment-Acute-Care-Toolkit-V1.1-2017.04.25.pdf
- The WAVR-21 Violence Threat Assessment App: https://www.resolver.com/apps/threat-assessment-software/

Security and Law Enforcement

Hospital organizations should allocate the appropriate resources and provide the necessary training to healthcare security leadership to prevent and respond to acts of violence on a hospital campus. Security professionals are integral members of the healthcare team who can help ensure a safe environment for employees and patients.

Training: Security should be trained on de-escalation efforts, appropriate use of restraints as last-resort patient management, policies and procedures in response to incidents, and incident reporting. There are several trainings and systems that are available, a few of which are incorporated in the Training and Education section of this guidance.

Security Technology: While there is a wide variety of technology available to healthcare security, organizations should determine what is most appropriate for their geography, demographics, current security controls in place, and existing risk assessments. Security technology should be custom designed to fit the risks inherent in the institution, with staff that are unbiased and not employed by a security technology supplier.

Law Enforcement: Hospitals should routinely meet with their local police departments to identify a hospital liaison for ongoing safety coordination efforts. In particular, hospitals should request assistance from law enforcement or an outside consultant to review possible risks based on prior incidents at or near hospital facilities (both on and off the campus) and the surrounding communities.

Healthcare Security Operations

Space Design for Security Technology

There are a variety of engineering controls hospitals have adopted based on known or identified risk of violence to employees, patients, and families/visitors. Examples of engineering controls that have been adopted in hospital settings are outlined below. These examples are provided for reference only as it is not possible for every hospital to provide or implement every practice that is outlined below given available resources and the physical structure of the hospital or service area. Hospitals should determine which practices could be considered based on the resources available, the atmosphere/culture within a specific service area, treatments being delivered, and applicability of the controls based on existing patient populations.

Security/Silenced Alarm Systems	Panic buttons, paging systems, or personal alarm devices that can be worn by employees Security silenced alarm systems
Egress Routes	Two exits for certain rooms, if applicable Safe room for employees during emergencies Furniture placement that allows clear and close exit routes, allowing for the caregiver to be closer to the door
Monitoring Systems & Natural Surveillance	Closed circuit video inside and outside the facility Curved mirrors Placement of nursing stations to allow for visual screening of areas Glass paneling in doors and walls Employees should know if video monitoring is in use of not and whether someone is always monitoring the video or not Employ crime prevention through environmental design(CPED), when possible
Barrier Protection	Deep counters at nursing stations Lock doors for staff and treatment rooms Keyless entry systems
Patient and Client Areas	Establish areas for patients and clients to de-escalate Provide comfortable waiting areas to reduce stress Divide waiting areas to limit spreading of agitation among clients and/or visitors
Furniture, Materials, Maintenance	Secure furniture and other items that could be used as weapons Replace open hinges on doors with continuous hinges Ensure locks on drawers with supplies that can be used as a weapon Pad or replace sharp edged furniture as able Reduce noise in certain areas Recess handrails, drinking fountains, and other protrusions
Lighting	Install bright, effective lighting inside and outside the facility, parking areas and walkways While lighting should be effective, it should not be harsh or cause undue glare
Travel Vehicles	Consider physical barrier between driver and patients Ensure proper maintenance of vehicles at all times
Access Control Systems	Systematic and consistent approach for the facility regarding access control systems should be designed based on vulnerability and other assessments of the facility

Policies & Procedures

It is the goal of every hospital to develop an environment of safety for healthcare staff and patients while still ensuring those operational practices, technologies, and the physical setup of a department does not create limitations for patients to access medically necessary care. While not an exhaustive list, below are examples of policies and procedures that have been adopted in many healthcare organizations to support healthcare violence prevention efforts.

Code of Conduct:

Hospitals should have an institutional code of conduct for all patients, visitors, and persons entering the facility or hospital premises that makes it clear that assaults are not considered "part of the job" or "inevitable" and that clear actions will be taken for incidents occurring. This code of conduct should be displayed prominently through signage and notices throughout the hospitals, in particular in high-volume patient and visitor areas. Hospitals should consider signage that includes visual symbols as well as plain language descriptions of the expected code of conduct.

Within this code of conduct, facilities should clearly state that the hospital is a weapon-free facility, and that treatment (with the exception of an emergency) may be delayed if there is a known weapon on a patient that may interfere with the ability to provide care. As stalking and intimidating acts are a continued concern, the code of conduct should also include language that video and photos of healthcare staff and patients are expressly prohibited without their permission and that of the hospital.

Physical and/or Property Searches on Patients and Visitors:

Hospitals should consider a standard policy for all locations that includes information on how and why searches for dangerous objects may be performed, patient participation and consent, how dangerous objects are handled, and how the search and results are documented within internal records and incident reports.

Searches should only be used as a measure to protect the safety of employees and patients when there is significant concern identified by the hospital staff that would require a search. We recognize that searches may result in patients feeling stigmatized and can lead to poor patient outcomes or a discharge against medical advice. Whenever possible, trauma and sexual assault history should be gathered before a search to minimize any distress to the patient. The MHA Workplace Safety and Violence Prevention Workgroup developed suggested criteria (See Appendix A) for a hospital process when conducting a search of a patient and/or visitor. This suggested criterion was reviewed by state regulators to ensure compliance with state regulations and licensure expectations.

Weapon Policy:

Hospitals are strongly encouraged to develop a policy and practice that informs patients, visitors, and others (e.g., law enforcement not acting within their jurisdiction) that the hospital is a weapon-free facility and weapons of any kind will not be allowed in a hospital location (on or off-campus locations), with an exception specifically provided for law enforcement officials (federal, state, or local) that are acting in an official capacity. Weapons of any kind that are identified or found should be held by hospital security professionals in a special secure area (or in a lockbox if available) and returned to the patient upon discharge as appropriate. In developing such a policy, hospitals should be aware that only licensed personnel are allowed to handle specific weapons (e.g. firearms) given the need for training in handling and removal of ammunition. As a result, hospital staff should be trained to know when to call security leadership to assist with securing and removing weapons. In the alternative, hospital staff should also be aware of the process for contacting local law enforcement, if there is a weapon and internal security leadership cannot be contacted.

Patient Screening:

Organizations may develop procedures to not only identify patients at risk of committing an act of violence, but also to manage the patient to reduce the likelihood that he or she will follow through with that risk. These procedures should include mechanisms for creating awareness of previous patient history of violent or assaultive behaviors in healthcare settings intent or contributing factors in previous incidents, potential patient triggers for aggressive behavior, and proven effective de-escalation techniques for clinical staff to use in developing a patient-specific violence prevention plan. The mechanisms may include the use of technology to track movements of identified at-risk patients and to notify appropriate staff of risk and patient plans when applicable. MHA is currently working with every acute care hospital to fully use the security alert function within the Collective EDie system adopted within the hospital electronic medical record system. The Collective EDie security alerts will push to emergency departments or directly to security if a patient presents at a different facility or returns to the same facility after previously displaying violent behavior. The system will allow hospitals to proactively align staff and other resources as appropriate to de-escalate patient behavior, and adjust the patient's environment to minimize risk. Please review Appendix B, which provides a detailed overview of the Collective EDie security alert system that is currently available to all acute care hospitals.

Entry or Exit Procedures:

Procedures established at the point of entry of a hospital can decrease risk and should include managing patient expectations within the waiting room, having sign-in procedures and visitor passes, and may include a process for identifying patients (in a non-discriminatory manner) with a history of violence, which can be shared among security, nurses, and admissions personnel. The Collective EDie is already providing this information to hospital emergency departments when a patient is admitted or registers for services.

Incident Response: Response Plans and Team:

Hospitals should have a response plan for incidents of violence, including immediate actions, de-escalation, response teams, and other actions as necessary based on the extent of the violent act.

Incident Record Keeping and Documentation:

Each episode of violence or credible threat to healthcare workers warrants a notification to leadership, to internal security, and, if appropriate, to outside law enforcement for assistance. An incident report should be created and used to analyze what happened and to inform actions that need to be taken to minimize risk in the future. Organizations should consider requiring that employees report all assaults and threats to a supervisor or manager, keep log books or reports of incidents for evaluation efforts, and advise employees of procedures for requesting police assistance or filing charges when they are victims of an assault. Employees should be made aware of what happens when incidents are reported and should be notified of the completion of an investigation and provided details if allowable and/or appropriate.

Classification of Incidents:

It is recommended that hospitals develop a uniform internal classification of incidents, including an opinion or assessment, if possible, of whether a patient intended to cause actual harm or whether the patient was not competent at the time due to his or her medical condition or his or her medication. Organizations can decide whether physician or clinical team input or medical notes are necessary for classification purposes on a case by case basis. Classification of incidents can help the appropriate staff investigate gaps in systems that could decrease the risk of such incidents in the future.

Post Incident Investigation and Reporting:

Post incident investigations are critical to ensuring safe guards are put in place to prevent similar events from occurring. Investigations should consider the following steps:

1. Report as required – Determine who needs to be notified within the organization and external to the organization when there is an incident, when incidents must be reported, information that needs to be included, and what other reporting requirements may be involved. (i.e., involvement of hazardous materials). This may include reporting to upper management, senior leadership, the board, or law enforcement;
2. Involve employees in the incident investigation – Employees who work most closely in the area where the event occurred may have insight into the causes and solutions;
3. Collect and review other information – Depending on the nature of the incident, records related to training, maintenance, inspections, audits, and past incident reports may be relevant to review;
4. Investigate near misses – Near misses are incidents where acts of violence are threatened but not completed, are caused by the same conditions that can produce more serious outcomes, and signal that some hazards are not being adequately controlled or that previously unidentified hazards exist;
5. Post incident notification - Victims should receive notice that the investigation has been completed, any conclusions if allowable or appropriate, and a list of resources to assist the individual with follow-up steps; and
6. Environmental assessment – Following an incident to determine if there are changes that need to be made to objects and/or operational structures to prevent their future use as a weapon or as a barrier for as a point of entry or exit (for staff, patients, visitors).

Hospitals are strongly encouraged to use a tracking system for incidents to help with current and future assessments. Examples of systems that are commonly used in hospitals include:

- Perspective or other incident reporting software
- RL Solutions
- Safe Spot
- Quantros
- Omnigo Software
- Guardtek
- Safety Event Reporting System (SERS)
- QED STARRS EMR
- Midas

Employee Support and Resources

It is recommended that employees who experience or are witnesses to incidents of violence are provided a comprehensive support system. This includes offering both medical treatment and psychological therapy (as needed), as well as information on the resources available to help the employee following the incident of violence. Organizations are encouraged to consult with internal groups such as human resources, occupational health, and other employee supports to identify available resources and supports that should be offered to employees. Organizations should also consider developing a policy to support an employee's return to work following incidents of violence that are consistent with federal and state requirements. Resources and supports that may be considered, as appropriate, include:

- Employee Assistance Program (EAP)
- Occupational Health
- Peer Support
- Crisis De-briefing
- Chaplain Services
- Office of Clinical Support/Psychiatry
- Employee Health Services
- Workers Compensation Program
- Assaulted Staff Action Programs (ASAP) for psychological support
- Outside Law Enforcement, if there is a need for criminal action

Care Coordination within the Care Continuum:

Hospitals should consider how information about prior incidents (including those patients who have a known high risk of violence) is communicated throughout the levels of care as the patient accesses inpatient, outpatient, and community-based services.

Training and Education

Training and education is critical to ensure awareness of existing policies and procedures and to provide employees with the tools needed to manage aggressive behavior for patients, visitors, and others coming into a facility. Training plans should be developed based on individual department and staff needs based on the safety and security hazards identified as part of the risk assessment.

Supervisors and management should be trained to not only recognize potentially risky situations but to make sure they are prepared to manage an incident, conduct intake when an employee reports an incident, and refer employees to services post incident as necessary.

Employees in identified high-risk areas of the organization should be trained in a manner meant to prevent or respond to violent incidents, as well as to assist with patient management, avoiding or preventing violence, de-escalation, and trauma informed care. There is no one-size-fits-all training program that will work in all areas of the hospital given the diverse operations and clinical services provided in locations that are both on and off the main campus of a hospital. It is therefore strongly encouraged that hospitals consult with hospital security leadership as well as the workplace violence prevention committee to determine what areas and types of training should be provided to various staff.

Elements of an effective and appropriate training program may include one or more of the following:

- Prevention and Incident Management
  - » Internal Violence Prevention program policies and procedures
  - » OSHA workplace training
  - » Risk factors of workplace violence
  - » Active Shooting Training
- Patient Management trainings
  - » Trauma informed care
  - » Recognizing escalating behaviors
  - » Defusing and de-escalating volatile situations
  - » Restraint application training

Depending on the learning objectives of each lesson or module, organizations should determine which trainings should be provided to all new employees as part of onboarding/orientation practices and annual training for employees, and which trainings should be delivered on demand or at other intervals for staff in high-risk departments.. Consideration should also be made to delivery methods to include a blended learning approach whenever possible to ensure highest level of participation across departments and personnel as necessary based on job functions and risk.

While there may be available funding from external sources to cover the cost of the trainings, hospitals should work through its workplace violence prevention committee to determine how to allocate appropriate resources to cover the cost of the trainings. Examples of external resources that may be available includes current insurance carriers for the hospital umbrella policies or grants from federal or state entities (e.g., Susan Harwood Training Grants https://www.osha.gov/dte/sharwood/index.html).

Hospitals in Massachusetts are using a variety of training resources, which include those listed below (listed in alphabetical order only):

- Alert Lockdown Inform Counter Evacuate (ALICE) training: https://www.alicetraining.com/
- AVADE training: http://avadetraining.com/
- Crisis Prevention Institute (CPI): https://www.crisisprevention.com/
- HDTS training: http://personalsafetytraining.com/healthcare-defensive-tactics-system/
- Management of Aggressive Behavior (MOAB): https://www.moabtraining.com/
- Stop the Bleed Campaign: http://stopthebleedingcoalition.org/

Program Evaluation

After the annual threat analysis is complete, facilities should consider how to use information collected to make necessary improvements and monitor success of efforts. Examples of internal practices that a hospital can take are listed below. It is not expected that hospitals should or can implement all of these practices as it will be based on the needs of the particular facility and the types of incidents that occur:

- Establishing a uniform violence reporting system for all staff and regular reviews of reports;
- Reviewing reports and information from staff meetings on safety and security issues;
- Analyzing trends and rates in illnesses, injuries or fatalities caused by violence relative to initial or baseline rates;
- Measuring improvement based on lowering the frequency and severity of healthcare violence;
- Conducting an internal analysis on the number of assault or attempted assaults with staff who have completed Management of Aggressive Behavior or other de-escalation trainings, to determine the efficacy of those trainings in reducing incidents for those staff and/or locations;
- Keeping up-to-date records of administrative and work practices to prevent healthcare violence to evaluate how well they work;
- Surveying workers before and after making changes within a facility, installing security measures or new systems to determine their effectiveness;
- Tracking recommendations from hospital committees through completion in actual operations;
- Keeping abreast of new strategies available to prevent and respond to violence in the healthcare and social service fields as they develop;
- Engaging staff periodically to learn if they experience hostile situations in performing their jobs;
- Evaluating the use of new security and/or operational changes with regard to preventing new or future incidents in certain departments or location; and
- Requesting periodic law enforcement or outside consultant review of the workplace for recommendations on improving worker safety.

Appendix A: Suggested Criteria to include in a Hospital Search Policy

Patient and/or Property Searches

Searches should be based on institutional policies that outline the clinical and/or safety reasons for conducting a search of the patient, their belongings, gifts brought to them, and/or their room upon admission, as well as upon returning from an authorized or unauthorized leave of absence/interrupted stay. This policy should include leaves for the day or shorter periods where a patient's clinical condition changes unexpectedly following their return to their inpatient level of care.

Hospitals should develop a specific process for determining when a search is appropriate. In particular, there should be a documented reason that would allow for a search, including reasonable suspicion by the hospital staff (clinical and administrative) that illegal, dangerous or potentially harmful items are being brought onto the hospital property. Examples of the items that could pose reasonable suspicion to include in a policy could be:

- Presence of medication or drugs that the hospital clinical staff has not prescribed;
- Illegal, dangerous or potentially harmful objects or intoxicating substances;
- Unauthorized hospital property or another person's property in their possession that poses a risk of harm to self, staff, or another patient;
- Information that the hospital has maintained that a patient, visitor, or other has a recent history of overdose or self-harm behavior;
- Demonstrating behavior (e.g. combative, verbally abusive or aggressive) that implies the patient may cause harm to self, staff, or another patient;
- Review internal security alerts regarding a patient's prior history of possessing illegal, dangerous, or potentially harmful objects, and/or whether the patient has exhibited prior aggressive/abusive behavior; these alerts should be incorporated into the hospital's own electronic medical record (EMR) using systems like the Collective EDie platform outlined in Appendix B.

Searches should not be more intrusive than necessary to accomplish the goal of protecting the patient, the hospital staff, and others. Hospital staff should contact security leadership within the hospital who should conduct the search. All searches should be performed with at least two staff present, one of which should be a security professional. Except in an emergency circumstance (as determined by the clinician or hospital staff), the patient must be informed as to the reason of the search, be asked for his or her permission to conduct a search in a voluntary and non-forcible manner, and, if possible and appropriate, be present during a search of their belongings, gifts, and/or room. For searches that occur in an emergency circumstance and for which the patient is not present during the search of property, the patient should be informed as soon as practical about the search. Healthcare providers should also consider policies that would allow a search without patient consent if there is an identified risk that warrants a search.

Whenever possible, trauma and sexual assault history should be gathered before a search. The search should be conducted in a way to minimize any kind of trauma to the patient.

Patients may not be restrained for a search unless it is determined by the hospital staff that they are an imminent threat to themselves, staff, or others. If restraint is necessary, a treating clinician should be consulted prior to the restraint and search, provided that an immediate search is necessary for the safety of the patient, hospital staff, and/or others. It is important to note that all hospitals are required to follow Medicare Conditions of Participation and The Joint Commission accreditation standards that also set criteria for a restraint and seclusion of a patient, so hospitals should consult with legal and other appropriate staff to ensure that a policy on restraint and seclusion of a patient takes these standards into consideration.

If a patient refuses a voluntary search, the hospital should follow its internal policies that may include confiscating any personal item(s) that may be a concern to hospital staff and placing it in a secure area (with other patient belongings) until discharge without further searching. A hospital may also want to consider such additional alternatives as requesting urine toxicology if a search is denied and there is a concern about potential opioid misuse and/or use.

Documentation of Searches

Hospitals should document as part of an incident report or through other internal records, which can be easily reviewed by appropriate staff and/or regulators if requested:

- the nature and reasons for a search; if it was for an emergency circumstance, then document the specific nature of the emergency;
- the names of the staff involved in the decision making to conduct a search, as well as who conducted the actual search;
- if the search is being done as part of the admission, an inventory and documentation of patients' belongings should be completed pursuant to hospital policy for admissions; and
- the results of such a search, including but not limited to:
- a description of any objects found,
- disposition if the object was harmful or dangerous to the patient, staff, or others, and;
- If the patient was not present during the search, the reasons for not being present.

Managing Contraband or Dangerous Objects

Caution should be advised when handling any illicit substance due to risk presented by accidental exposure to substances such as fentanyl or paraphernalia such as needles. It is recommended to have a minimum of two staff present at the search, one of whom could be a security officer. Hospital staff should also conduct the search in the presence of the patient and/or family, if available and appropriate.

Objects or substances that present a safety concern to the patient and/or others should be removed. The item should be stored in a secure area until the patient is discharged pursuant to hospital policies for storing patient possessions, or destroyed if the substance poses a safety concern to the patient, hospital staff, and/or others, including other patients.

Removal of Clothing

It is well recognized that removal of clothing may be necessary to enable an appropriate medical screening examination for the identification of an emergency medical condition. Another reason to request the removal of clothing is to protect self or others against potentially harmful substances or weapons that might be hidden on a patient's person. Forced removal of clothing is a form of physical restraint, and as such, all alternatives to this action should be used before forced removal of clothing.

Therefore, compelling clinical information indicating imminent risk to self or others is necessary to prompt forced removal of clothing.

All hospital policies regarding clothing removal should recognize the right of patients to refuse to remove their clothing (as well as the need by the clinician to request the removal of clothing if appropriate to conduct a medical screening examination). This right should be included in any materials or communications presented to patients that enumerate their rights. Patients need not be verbally informed of this right prior to a request for the removal of clothing, but they must be informed of this right if the patient refuses the request for removing their clothing.

If a search of the person is conducted, which may also include the removal of any clothing beyond the outer clothing, one of the two staff present should be a clinician. Such searches should be done in a private or secure location. All clothing should be returned to the patient as soon as is reasonable.

Hospital policies regarding clothing removal should apply equally to all patients seeking treatment in the hospital. Policies should not be developed that focus on clothing removal or pat downs for targeted patients (such as those being admitted for mental health or substance use disorder treatment).

Visitor Searches

Searches of visitors should also be conducted consistent with institutional policies or those recommendations outlined above, and should occur if:

- There is a reasonable suspicion of presence of contraband,
- A patient's clinical condition changes unexpectedly following visitation, or
- The patient, staff, or others are in immediate risk of harm.

For visitors suspected of using illicit substances in the hospital (based on known previous history of drug misuse while on or off the hospital property):

- For locked psychiatric units, all packages from visitors should be checked in with a nurse or security professional first to ensure safety of the patient and employees, and
- A reasonable suspicion of bringing in unapproved items (for example paraphernalia), illegal substances, or non-prescribed opioids may necessitate a search of a visitor's belonging.

To ensure best possible care for the patient, a hospital should use these procedures to ensure that the patient has no objects which may be harmful or dangerous to the patient, staff, or others including those brought in by visitors. If there is reasonable suspicion that a visitor is providing a patient with objects which are harmful or dangerous to the patient, staff, or others, steps must be taken to prevent misuse and potential harm to patients and/or others. If the visitor refuses a search, indicate that visitation privileges may be terminated or limited.

Appendix B: Implementing Security Alerts within Hospital EMRs

Introduction

Violence in healthcare has become a significant public health issue and of great concern to hospitals and health systems whose mission is to make their communities and workplaces healthier and safer. One solution in violence prevention is developing and implementing internal systems that provide critical clinical and operational information for better management of encounters with patients at high risk for security or safety incidents. The Collective EDie platform already in use in the majority of hospitals is key to meeting this solution.

What is Collective EDie?

The Collective EDie application connects EDs across geographies. When a patient registers in any participating ED, Collective is alerted and queries available ADT and other data repositories (such as MassPAT) to identify in real-time whether the patient meets any pre-defined risk criteria. If risk is identified, Collective will automatically push a notification to the ED. These notifications are designed to give the ED provider a quick-to-read, easy-to-digest integrated clinical snap shot of the presenting patient, including a summary of risks identified (e.g., security, opioid), critical clinical information (e.g., recent ED or inpatient encounters, existence of ED care recommendations from other providers), and important care coordination information (e.g., other members of the patient's care team, existence of an existing pain contract for the patient).

Understanding Security Alerts provided within Collective EDie:

The Security Events section provides a space where users may document when a patient has posed a security threat to care providers, clinical staff or other patients during an appointment or visit, as well as review a patient's previous security events. Collective EDie is configured at all hospitals to trigger an alert based on security events that have been captured within the tool anywhere across the network of participating healthcare systems. When a patient with a past security event presents at an ED, a notification will push details about the security event to hospital security (non-clinical content) or the ED provider(s) and staff, allowing hospital staff to take proper precautions prior to and during that patient encounter. Because the security alerts are located within real-time notifications, as well as accessible in the web-platform, staff can be assured that those patients that may pose the most threat for workplace violence are quickly identified.

Examples of Security Events provided in current Collective EDie notifications include:

EXAMPLE 1:	Patient was verbally abusive towards care providers, staff or patient. Patient verbally threatened care providers, staff or other patients.
	Details within the Notification: The patient made gestures with his hand that he was going to shoot security. Security notified the local PD officer while keeping eyes on the gentleman. The gentleman proceeded outside and waited for security to follow. The gentleman took off his shirt and informed security that he was ready to fight. The green unit arrived and the gentleman departed the area after seeing the local PD arrive.
EXAMPLE 2:	Patient threw objects at a care provider, staff or patient.
	Details within the Notification: Medical staff requested the standby because the patient was being verbally abusive and had thrown her food tray at staff before they called security. Security stood by as the PA talked with the patient. Once the patient had calmed down enough for medical staff, security vacated the area.
EXAMPLE 3:	Patient was verbally abusive towards care providers, staff or patient.
	Details within the Notification: Patient was discharged and was found harassing, screaming, yelling, and cursing, at staff during shift change. 2 officers and 1 PD officer responded and escorted the individual off property.

Many hospitals who are successfully using Collective EDie Security Events are receiving their direct Collective EDie Security Event Alert directly to their security staff or their triage desk. Here are a few successful workflows:

1. Send a Collective EDie alert directly to hospital security via email or text. These alerts do not include medical information and are tailored to only have the past security event information.
2. Use specific icons in your EMR to differentiate between security alerts and alerts being received based on clinical risk criteria. Some hospitals have chosen a red exclamation point but any icon will work if it is easily recognized by your providers and hospital staff.
3. If your hospital is not currently setting up an electronic integration, hospitals can have their security event notifications go to a network printer at the Triage desk that has a tray set up with brightly colored paper such as neon pink or yellow. Staff and providers should be trained to understand that this means this patient has a Collective EDie security event.

Collective Medical will work with each hospital to identify and set up the best workflow to meet the needs of their hospital and ensure that Collective EDie security events are easily identified and communicated within the emergency department.

General Tips on Creating Security Events

- **Identify users that will be responsible for updating the security events in Collective EDie.** Your hospital may already have a plan in place for reporting security events; if so, this may be applied to reporting events in Collective EDie. Most commonly, security events are entered in Collective EDie by an ED Case Manager or a designated ED Nurse.
- **Associate the security event, when appropriate.** For most patients, you will be able to associate an event as having occurred during a specific visit to your facility. Associating the event with a visit will allow others to understand how recently this event occurred.
- **Identify the type of security event that transpired.** Denoting the type of security threat will allow others to immediately assess the threat level when a patient presents at subsequent visits.
- **Add additional details when relevant.** It can be useful to provide context for the event, including triggering items that led to the event, or action plans for subsequent visits. For example, it may be helpful to note that a patient escalates after being denied prescriptions or that a patient must have multiple staff members in the room during treatment.
- **Enter the security event in Collective EDie within 24 hours of the event.** If possible, enter the event within an hour of the visit. There have been many instances where a patient has visited multiple EDs in a single day. Please provide this information to other hospitals in a timely manner.
- **Do not use any pejorative language towards a patient in a security event.** Please remember to show respect to your patients even when the patient has shown destructive behavior.

Maintaining Privacy and Security in Usage of Security Alerts Information

Collective treats all information as highly sensitive patient health information and as such, employs several essential privacy and security controls.

- First, Collective only accesses security alert information to analyze risk and pull information into ED notifications, it does not use the data for any other purpose, and the information is not stored in any CMT database.
- Second, Collective delivers the security alert to ED providers as part of a notification. Hospitals may save the notification (including security alert) as a clinical note in the patient's medical record, but hospitals may not extract, store or manipulate the security alert included in the Collective EDie notification.
- Third, Collective employs end-to-end encryption of all data as it transmits through the CMT infrastructure and enters the hospital's clinical information systems.

For any further questions you may have:

Collective is happy to provide additional information or documents and/or answer any questions about the Collective EDie Security Alerts that are already available within your hospital EMR. Please contact Collective's General Manager of the Northeast, David Kimball at (801) 473-8848 or by email at David.Kimball@collectivemedical.com.