Behavioral Threat Assessment and Management: Prevent and Protect

A Resource Compendium for Further Learning

www.aha.org/hav

American Hospital Association
Advancing Health in America

www.fbi.gov/prevent

Table of Contents

Introduction 3

Threat Assessment and Management in the Real World:
The University of Virginia Medical Center 4

The Importance of Training on Risk Factors, Warning Signs and Pre-attack Behavior Indicators: What Health Care Workers Need to Know to Prevent Targeted Violence 6

Why a National Guide Is Needed for Violence Prevention in Hospitals 11

Vulnerabilities in the Patient Care Cycle: Utilizing a Proactive Approach in Mitigating Affective Violence 13

The Pathway to Targeted Violence: Predatory Behavior, Shame and the Thin Line Between Suicide and Homicide 17

The Importance of Behavioral Threat Assessment and Management 23
for Hospitals and Health Systems

Best Practices in Building and Supporting Threat Management Teams 31

Effective Use of BTAM in Health Care Settings 35

Building Behavioral Threat Assessment and Management Teams Within Hospital Settings... 38

Legal Considerations for HIPAA and BTAM Teams in Hospitals:
Working with Law Enforcement While Following HIPAA 40

Law Enforcement BTAM Teams: What Hospitals Should Know 45

A Mental Health Perspective: Overcoming Barriers to Working With Law Enforcement........ 47

Bystanders: An Overlooked Resource 52

Don't Forget EMS and Fire: The Importance of Nontraditional Partners in BTAM 53

Suggested Citation:

Gibson, K., Tillman, J., Koch, H. M., Stormer, M., Desrosiers, C., Fein, R., Saathoff, G., Gray, A., Jones, N. T., Markowski, E., Muck, A., Newring, K. A. B., Rowe, S., Rozel, J., Scalora, M. J., Van Male, L., and Winternheimer, J. (2026). Behavioral Threat Assessment and Management: Prevent and Protect | A Resource Compendium for Further Learning. Chicago, IL; American Hospital Association and Federal Bureau of Investigation.

Disclaimer: The views and opinions expressed in this resource are those of the expert authors and do not necessarily reflect the official policy or position of the American Hospital Association. The content is provided for informational purposes only and does not constitute legal advice.

Introduction

This document presents 14 distinct chapters on implementing behavioral threat assessment and threat management (BTAM) strategies within hospital settings. Its purpose is to provide a comprehensive overview of approaches aimed at reducing violence and preventing threats from escalating into harmful actions.

The authors, recognized by the FBI's Behavioral Analysis Unit (BAU-1) as leaders in the field, bring expertise from security, legal and law enforcement backgrounds, offering practical insights and multidisciplinary strategies tailored for health care environments. In 2010, BAU-1 created the Behavioral Threat Assessment Center, which is the only national-level, multiagency, multidisciplinary task force in the federal government focused on the prevention of terrorism and targeted violence. As part of the FBI's efforts to address threats of targeted violence through prevention and early intervention, BAU-1 established the National Threat Assessment and Threat Management (TATM) initiative to educate, lead and support the incorporation of BTAM principles into FBI investigative operations. To further their prevention efforts and expand their TATM initiative, BAU-1 partnered with the American Hospital Association (AHA) for the combined goal of promoting violence prevention.

This resource, which is especially valuable for health care security professionals seeking to deepen their understanding and sharpen their ability to respond effectively to threats within their organizations and communities, serves as the complement to the leadership guide, Behavioral Threat Assessment and Management: Prevent and Protect, A Leadership Guide for Preventing Targeted Violence in Health Care Settings, created by the AHA and the FBI BAU-1. The guide distills and summarizes the key insights from the original 14 expert perspectives to make them accessible for health care leaders. By translating complex BTAM strategies into clear, actionable guidance, the leadership guide helps executives and decision-makers understand the essential elements needed to strengthen safety and preparedness across their organizations.

Threat Assessment and Management in the Real World: The University of Virginia Medical Center

Andrew Muck, M.D.
Chair and Professor of Emergency Medicine at the University of Virginia

Ed Markowski
Director of Threat Assessment at the University of Virginia

Gregory Saathoff, M.D.
Professor, Department of Emergency Medicine & Public Health Sciences School of Medicine at the University of Virginia

Emergency medicine and emergency departments have always had a long-standing interest in threat assessment and threat management, both of which are vital to an emergency department. As the face of a health system, the emergency department regularly interacts with patients who are experiencing mental health or toxic ingestion-related conditions. If a crisis happens anywhere in the health system, the emergency department is often expected to respond and be prepared to receive patients from any incident. With an open door and 24/7 service, the emergency department is a soft target for those who may wish ill on a community. As a high stress environment, it is not beyond consideration that a worker within the emergency department can find themselves in crisis. The emergency department also recognizes how little can be accomplished without a robust medical center approach, response and prevention mechanism for threat assessment and management.

The University of Virginia (UVA) Medical Center uses the latest understandings and systems of the Behavioral Threat Assessment and Management concepts to keep our staff and patients safe. UVA Medical Center's comprehensive Threat Assessment and Management Program ensures the safety and well-being of its patients, staff and visitors. This program is designed to identify, assess and manage potential threats through a multidisciplinary approach, combining expertise from medical, security and psychological fields. The goal is to create a safe and secure environment conducive to health care excellence and patient recovery.

Since 2008, the Commonwealth of Virginia has required all public institutions of higher education to have violence prevention committees and threat assessment teams. At the University of Virginia and its Medical Center, the Office of Threat Assessment oversees this committee and team. The threat assessment team has staff from the Department of Psychiatry and Neurobehavioral Sciences; Patient Safety Risk Management; the Office of Threat Assessment; the university police department; Human Resources; Student Affairs; the Office for Equal Opportunity and Civil Rights; counseling and psychological services; the Faculty and Employee Assistance Program; and university counsel. The mission of the threat assessment team is to assess, manage, intervene and mitigate threats in a multidisciplinary approach by coordinating, investigating and mitigating violence.

The University of Virginia Medical Center relies heavily on the multidisciplinary team and the specific areas of expertise therewithin. Having such a team allows specific aspects of all parties to be treated with dignity and respect. Special privacy aspects of medical information must be adhered to and honored. Privacy and appropriate latitude are carefully observed so as to not compromise HIPAA compliance.

Program Structure and Components

The Threat Assessment and Management Program at UVA Medical Center operates under the UVA Department of Safety and Security with a structured framework that includes several key components:

- **Threat Assessment Multidisciplinary Teams.** Comprising professionals from various departments such as security, mental health, human resources, and legal, the multidisciplinary teams meet to review and assess threats. This program is responsible for developing and implementing intervention strategies and coordinating with law enforcement when necessary. The Situational Awareness of Violent Events (SAVE) teams are exemplary components of this program.

- **Reporting Mechanisms.** A robust reporting system allows staff, patients and visitors to report potential threats anonymously. Reports can be made through hotlines and online portals or directly to security personnel. Immediate response protocols are in place to address urgent threats. Multidisciplinary teams review the cases, and case workers are assigned to those individual cases.
- **Risk Assessment Tools.** The program utilizes evidence-based risk assessment tools to evaluate the seriousness of reported threats. These tools help determine the likelihood of a threat being carried out and the potential impact, allowing the threat assessment and management programs to prioritize resources and responses effectively.
- **Training and Education.** Education and training sessions are available in person and online for hospital staff to recognize warning signs of potential threats and appropriate responses. These sessions cover conflict resolution, de-escalation techniques and emergency response procedures. Education extends to patients and visitors, informing them of how to report suspicious activities.
- **Preventive Measures.** Proactive measures such as environmental design modifications, security presence enhancement and access control systems are implemented to prevent threats. These measures are regularly reviewed and updated based on evolving security needs and technological advancements. The goals of such preventive measures include recognizing and promoting protective factors, minimizing trigger events, and protecting potential targets.

Procedures and Protocols

When a threat is identified, a systematic procedure is followed:

- **Identification and Reporting.** The first step is the identification and reporting of the threat. This can be done by any member of the hospital community through established reporting mechanisms. Threat assessment teams can be contacted whenever someone observes a statement, behavior or situation that creates concern. Information can be reported to the Office of Threat Assessment or the University police department.
- **Initial Assessment.** The Threat Assessment Team performs an initial assessment to determine the credibility and severity of the threat. This includes gathering information and evidence from the reporting party and witnesses.
- **Detailed Investigation.** A detailed investigation is launched for all credible threats. This involves coordination with law enforcement, review of available information, and interviews with relevant individuals.
- **Intervention and Management.** Based on the assessment, the Threat Assessment and Management Program develops an intervention plan. This may include increased security measures, counseling or mental health support for the individual posing the threat, or legal actions if necessary.
- **Follow-up and Monitoring.** Continuous monitoring and follow-up ensure that the threat is effectively managed and that any residual risks are mitigated. The team regularly reviews cases to update intervention strategies and improve the program's effectiveness.

Conclusion

The Threat Assessment and Management Program at the University Hospital of UVA Medical Center is a vital component of the institution's commitment to safety and security. By leveraging a multidisciplinary approach and utilizing advanced assessment tools and preventive measures, the program aims to proactively address and mitigate threats, ensuring a safe environment for all. Continuous education, rigorous procedures and a responsive Threat Assessment Team are the cornerstones of this comprehensive program, reflecting UVA Medical Center's dedication to excellence in health care and safety.

The Importance of Training on Risk Factors, Warning Signs and Pre-attack Behavior Indicators: What Health Care Workers Need to Know to Prevent Targeted Violence

Mario J. Scalora, Ph.D.
Professor of Psychology and Director of the University of Nebraska Public Policy Center
University of Nebraska-Lincoln

The contributions in this document provide a rich background regarding the nature and extent of the complex challenges inherent in addressing workplace safety within the health care sector. Before addressing the nature of training to support safety efforts, it is important to recognize the range of risks to be addressed, as well as challenges faced by stakeholders in reporting and sharing safety-related concerns.

Proper training needs to consider the various sources from which the risk of workplace violence could emerge. As a service delivery sector, the health care industry is not alone in having to manage workplace violence risks from a range of sources, including:

- Criminal intent from external parties (e.g., theft, sexual assault)
- Client/customer-driven violence (e.g., agitated/disgruntled clientele or family members)
- Insider risks from co-workers (e.g., grievance between co-workers, workplace discipline, possible/pending termination)
- Domestic violence (directed toward clients or co-workers) intruding upon the workspace
- Extremist/issue-driven grievances (e.g., conflicts over policies related to controversial issues

Frequently, training may focus on one type of risk, often emanating from patients or families during clinical situations, and may therefore neglect attention to other potential sources of violence.

Noteworthy Lessons from Prior Acts of Workplace Violence

Bystanders may have observed concerning behavior prior to incidents of targeted violence but did not report them to public safety officials or employers who could have engaged in protective actions.[1,2] This is particularly true in health care settings, in which a substantial amount of workplace violence and harassment incidents are underreported.[3]

It is critical when building a workplace violence prevention training strategy not just to focus on disseminating warning sign information but also to facilitate continuous outreach to stakeholders and partners utilizing empowerment-based strategies consistent with an organizational culture of safety.[4,5] Given the persistent underreporting of concerning behavior, significant efforts are needed to build trust across key stakeholders. An integrated workplace safety strategy is consistent with a culture of safety that protects both patients and workers from harm and injury.[6] As a result,

1 Meloy, J. R., Hoffmann, J., Guldimann, A., & James, D. (2012). The role of warning behaviors in threat assessment: An exploration and suggested typology. *Behavioral Sciences & the Law, 30*(3), 256-279.

2 Meloy, J. R., & O'Toole, M. E. (2011). The concept of leakage in threat assessment. *Behavioral Sciences & the Law*, 29(4), 513-527.

3 American Nurses Association. (2019). Issue Brief: Reporting Incidents of Workplace Violence. https://www.nursingworld.org/globalassets/practiceandpolicy/work-environment/endnurseabuse/endabuse-issue-brief-final.pdf

4 Kim S., Kitzmiller R, Baernholdt M, Lynn MR, Jones CB. (2023a). Patient Safety Culture: The Impact on Workplace Violence and Health Worker Burnout. *Workplace Health & Safety*. 71(2):78-88. doi:https://10.1177/21650799221126364

5 Kim, S., Lynn, Mary R. PhD, RN; Baernholdt, Marianne PhD, MPH, RN, FAAN; Kitzmiller, Rebecca PhD, MHR, RN-BC; Jones, Cheryl B. PhD, RN, FAAN. (2023b). How Does Workplace Violence–Reporting Culture Affect Workplace Violence, Nurse Burnout, and Patient Safety? *Journal of Nursing Care Quality* 38(1):p 11-18, | DOI: 10.1097/NCQ.0000000000000641

6 U.S. Department of Labor. (n.d.). DOL Workplace Violence Program. Office of the Assistant Secretary for Administration & Management, U.S. Department of Labor. https://www.dol.gov/agencies/oasam/centersoffices/human-resources-center/policies/workplace-violence-program.

training should integrate policies and strategies that promote awareness of and protection from a range of physical and psychological risks, including workplace violence. Organizations that facilitate a culture of safety are more successful in gaining stakeholder engagement and trust in procedures.[7,8] The culture of safety mindset incorporates extensive communication related to processes, leadership and management support for reporting, as well as nonpunitive approaches to employee errors that may occur. Employees need to observe a consistent leadership response to safety concerns that aligns with the training protocol. Health care and security leadership cannot assume that trust is adequately pre-established among personnel. Researchers[9,10] highlight the positive role of employee engagement and workplace culture when influencing willingness to respond to workplace violence. Kim and colleagues reinforced that higher levels of patient safety culture were associated with fewer experiences with workplace violence.[11]

Barriers to Reporting

The literature on the range of factors that inhibits reporting concerning behavior extensively emphasizes the need for consistent reinforcement of safety principles.[12,13,14,15,16,17] Training content must recognize these barriers and the organizational supports and processes that will mediate the potential impediments to reporting. Such barriers may result from both psychological and organizational sources.

Personal or psychological factors inhibiting reporting of concerning behavior may include:

- Fear for personal safety (e.g., retaliation from the person of concern).
- Fear of being viewed as overreacting by management or colleagues.
- Fear of being viewed by colleagues or management as incompetent or unable to deal with difficult situations.
- Fear of potential retaliation for reporting internal workplace harassment or bullying.
- Ignorance of reporting procedures or who to contact.
- Disbelief that the concerning behavior (e.g., threat of violence) could materialize.
- Having a visceral reaction to life safety being threatened.

Organizational barriers to reporting could include:[18,19,20,21]

- A perception that workplace violence is "part of the job."
- Limited institutional policies or procedures.
- A perception that the concerning behavior happens so frequently that it's burdensome to report.

---

7 Kim S., et al. Patient Safety Culture.

8 Kim S., et al. Workplace-Violence Reporting Culture.

9 Ibid.

10 Saleem, Z., Shenbei, Z., & Hanif, A. M. (2020). Workplace Violence and Employee Engagement: The Mediating Role of Work Environment and Organizational Culture. *Sage Open*, 10(2). https://doi.org/10.1177/2158244020935885

11 Kim S., et al. Patient Safety Culture.

12 American Nurses Association. Reporting Incidents of Workplace Violence.

13 Blando J, Ridenour M, Hartley D, Casteel C. Barriers to Effective Implementation of Programs for the Prevention of Workplace Violence in Hospitals. (2015). *Online Journal Issues Nursing*. 20(1); Epub 2014 Dec 4. PMID: 26807016; PMCID: PMC4719768.

14 Copeland, D. & Henry, M. (2017). Workplace Violence and Perceptions of Safety Among Emergency Department Staff Members: Experiences, Expectations, Tolerance, Reporting, and Recommendations. *Journal of Trauma Nursing*. 24(2):p 65-77. | DOI: 10.1097/JTN.0000000000000269

15 Hatch-Maillette, M.A., Scalora, M. J., Bader, S.M., & Bornstein, B. (2007). A Gender-Based Incidence Study of Workplace Violence in Psychiatric and Forensic Settings. *Violence and Victims*, 22, 449-462.

16 Kim S., et al. Workplace-Violence Reporting Culture.

17 Low, E. C., Scalora, M. J., Bulling, D. J., DeKraai, M. B., & Siddoway, K. R. (2024). *Journal of Threat Assessment and Management*, 11(1), 19-31. https://doi.org/10.1037/tam0000202

18 American Nurses Association. Reporting Incidents of Workplace Violence.

19 Blando J., et al. Barriers to Effective Implementation.

20 Copeland, D., et al. Workplace Violence and Perceptions of Safety.

21 Kim, S., Lynn, Mary R. PhD, RN; Baernholdt, Marianne PhD, MPH, RN, FAAN; Kitzmiller, Rebecca PhD, MHR, RN-BC; Jones, Cheryl B. PhD, RN, FAAN. (2023b). How Does Workplace Violence–Reporting Culture Affect Workplace Violence, Nurse Burnout, and Patient Safety? *Journal of Nursing Care Quality* 38(1):p 11-18, | DOI: 10.1097/NCQ.0000000000000641

- Challenging or complex reporting procedures that create a disincentive for reporting.
- A perceived lack of organizational response or support when concerning issues are reported.
- Fear that reporting will reflect poorly on the staff member (e.g., perceived inadequate performance, victim blaming).
- Belief that some patients will not be held accountable for their violent actions (e.g., persons with dementia, persons with serious mental illness).
- Limited agreement on definitions of violence (including threats or harassment).
- Belief that reporting will not change the situation or decrease the potential for future incidents of violence.
- A perception that the incident was not serious enough or worth the effort to report.
- Lack of training related to reporting and managing workplace violence.
- Co-workers' worry that the person of concern may receive an unnecessary punitive response.

Key Values That Promote Safety

All key stakeholders (e.g., direct care staff, support personnel, leadership) need to be educated and trained regarding violence prevention policies and processes. Regardless of audience, certain key values and expectations should be an integral part of the training. To assist with addressing the impediments to reporting detailed above, training must therefore highlight the following values consistent with a culture of safety mindset:

- Safety activities should reinforce the value of prevention, as well as maintaining dignity and respect for all parties, during the assessment and management of concerning behavior.
- Supportive and nonpunitive strategies will be used as appropriate in response to reports of concerning behavior, emphasizing the ability to assist parties and de-escalate grievances that may emerge.
- Reports of concerning behavior will be handled with discretion and confidentiality, as appropriate, to maintain the safety of the reporter as well as the dignity of all parties involved.
- All reports of problematic behavior will receive appropriate attention to address safety and related concerns.
- Everyone within the organization has the responsibility and obligation to support organizational safety.

The 'Musts' of Leadership-level Training

Address barriers to reporting. Training at the leadership level should directly address barriers to reporting concerning behavior. The literature suggests that bystanders and victims often prefer informal reporting processes via different gatekeepers (e.g., colleagues, supervisors, etc.), which highlights the need to support both formal and informal reporting of concerning behavior.[22,23] All organizations should have trained gatekeepers, regardless of their job title, who may be approached by colleagues with concerns.

At the employee and direct care level, training should address the potential barriers to reporting and how the organization will promote the reporting of concerning behavior. Employee training should also highlight the value of encouraging anyone still hesitant to utilize formal reporting mechanisms to approach trusted colleagues who can provide them with support. Finally, employees and direct care staff should be provided with a range of reporting options, including anonymous avenues, to address concerns.

In addition to the warning behaviors listed below, management and leadership staff should be trained at a general level on how concerning behavior might be assessed and managed in order to reassure apprehensive staff of the supportive aspects of the process.

Positively reinforce reporting. Leadership and management training should cover key aspects of responding to reports of concerning behavior, as the response to reports is critical to enhancing stakeholder trust and minimizing

---

22 Hatch-Maillette, M.A., et al. Gender-Based Incidence Study.

23 Low, E. C., Scalora, M. J., Bulling, D. J., DeKraai, M. B., & Siddoway, K. R. (2024). Journal of Threat Assessment and Management, 11(1), 19-31. https://doi.org/10.1037/tam0000202

reporting barriers. This aspect of training should emphasize ways to positively reinforce reporting and create a culture where reporting concerns is viewed as a positive action staffers can take. *Always, always, always positively reinforce reporting a concern.*

- Reporters may require follow-up regarding the level of concern/risk determined for the problematic behavior as well as organizational response.
- It is also an opportunity to share potential safety planning tips, including possible strategies to monitor and address future situations.

Know the range of workplace violence risks. Training for all stakeholders should, at least briefly, review examples of the range of workplace violence risks, including:

- Criminal intent from external parties (e.g., theft, sexual assault).
- Client/customer-driven violence (e.g., agitated/disgruntled clientele or family members).
- Insider risks from co-workers (e.g., grievance between co-workers, workplace discipline, possible/pending termination).
- Domestic violence (directed toward clients or employees) intruding upon the workspace.
- Extremist/issue-driven grievances (e.g., conflicts over policies related to controversial issues).

Recognize the warning signs of behaviors of concern. All key parties within the organization should receive information periodically regarding potential behaviors of concern. It is strongly encouraged to provide staff with multiple reminders across different modalities (e.g., face-to-face and/or online training, reminders on websites, email) and not rely on single or required annual training events. Repetition is important, as employees can easily forget details from even the most effective training when under stress from a challenging situation.

While it is important to share a range of examples of concerning behavior, it is just as important to keep it simple. Generally, stakeholders recognize when they are concerned about something but may be unsure about reporting. As a result, all stakeholders should be encouraged to report *anything* that raises fear or concern. The training should reinforce the notion of *"See something, say something, do something now"* when encountering safety concerns.

Regardless of source, potential behaviors of concern and warning signs include:[24,25,26,27,28]

- **ANYTHING THAT RAISES FEAR OR CONCERN.**
- Any behavior that threatens safety.
- Activity or statements of an aggressive or threatening nature.
- Behavior that is escalating or becoming increasingly threatening/aggressive.
- Showing interest in or referencing violent acts or imagery such as potential violence, recent acts of violence, perpetrators of violence, weapons or extremist groups.
- Concern about potential sabotage or theft, or unauthorized access to sensitive information/material.
- Escalating a grievance toward a person or the organization, or blaming colleagues or the organization for their grievance.
- Leakage of intent (e.g., verbally, online) to perform violence.
- Expressing violence as an option for their problems.
- Disruptive workplace behavior.

24 American Nurses Association. Reporting Incidents of Workplace Violence.

25 Gallant-Roman, M.A., (2008). Strategies and Tools to Reduce Workplace Violence. *AAOHN Journal*, 56:11, 449-454.

26 Hatch-Maillette, M.A., et al. Gender-Based Incidence Study.

27 Meloy, J.R., et al. The role of warning behaviors.

28 Meloy, J.R., et al. The concept of leakage.

Train for engaging with challenging populations. Staff violence prevention training would also benefit from attention to strategies to address potentially challenging behaviors or issues, particularly from persons demonstrating agitation, symptoms of substance abuse or signs of serious mental illness.[29,30,31] Violence could be more frequently encountered by staff working with various populations, including patients with conditions such as delirium, dementia, traumatic brain injury, psychotic disorders or drug/alcohol intoxication. Workplace violence prevention training can also be later supplemented with de-escalation training to manage problematic, agitated or grievance-driven behavior with challenging populations, as well as to familiarize staff with available safety processes (e.g., duress notification, summoning assistance, situational awareness).[32,33,34]

Conclusion

Workplace violence prevention training must be approached from a holistic level to support a safety culture that reinforces the reporting of concerning behavior across all levels of the organization. Such training should review the organizational values that facilitate reporting, as well as directly address barriers to disclosing concerning behavior. In addition to face-to-face training, safety-related processes and information should be reinforced periodically across multiple channels. Highlighting the need for multiple reporting channels, including informal gatekeepers, is paramount.

Training related to concerning behavior and warning signs should, in a straightforward manner, broadly reinforce that stakeholders should report *anything that raises fear or concern.* Significant attention from organizational leadership and management bolsters efforts to address reporting barriers, as well as provides consistent and meaningful support to stakeholders who report concerning behavior. Trust among stakeholders is strengthened when organizational actions demonstrate a meaningful partnership addressing safety.

29 Blando, J., et al. Barriers to Effective Implementation.
30 Kim, S., et al. Workplace Violence-Reporting Culture.
31 Kim, S., et al. Patient Safety Culture.
32 Blando, J.,et al. Barriers to Effective Implementation.
33 Kim, S., et al. Patient Safety Culture.
34 Kim, S., et al. Workplace Violence-Reporting Culture.

Why a National Guide Is Needed for Violence Prevention in Hospitals

Gregory Saathoff, M.D.
Professor, Department of Emergency Medicine & Public Health SciencesSchool of Medicine at the University of Virginia
Forensic Psychiatrist, Consultant, FBI BAU-1

Targeted violence threatens all environments within our society. In my faculty role within our School of Medicine, as well as my forensic psychiatric position within the FBI's Behavioral Analysis Units (BAUs), I have witnessed a dramatic evolution in targeted (predatory) and affective violence over the last four decades, and am aware that such significant change is not unique to our university health system. Just as the U.S. Department of Justice and the FBI saw the need to collaborate with law enforcement and educators for a national guide for schools 25 years ago, resulting in the BAU"s publication of a national guide for schools, so too is this a time to recognize with the American Hospital Association a similar obligation to America's hospitals.[35] With the essential aid of BAU partners, multiple potential incidents of school violence have been prevented due to effective collaboration between stakeholders. Through assessments of countless cases, best practices have been developed that can help inform and protect the unique hospital and health care environments and the people who work within them.

As places that serve the public's most compelling concerns of life and death — and the emotions that are associated with such high-stress situations — hospitals have long been understood to be at risk for violence. Indeed, the need for violence prevention is not a new problem for America's hospitals, and in fact is a global problem. The presence of security staff and thoughtful design of the hospital environment can provide both the human interface and architecture that may serve to mitigate violence.

The causes of violence are complex. Evolving societal realities that drive violence further fuel that complexity and, therefore, the challenges that we face. Just as modern hospitals are built to physically evolve according to changing needs, so too must our understanding of violence prevention needs for hospitals.

The U.S. system of medical and nursing education has long set the standard for other nations. Advances in critical care medicine and a decrease in average hospital stays (as well as readmissions) are examples of the metrics of success and increased efficiency within modern medicine. Patient privacy protections through the Health Insurance Portability and Accountability Act of 1996 have had a powerful impact within health care and have been beneficial in serving the needs of patients.

We have also seen an avalanche of medical information readily available to the public. The benefits of a more educated patient population are obvious; however, easy access to information came with an explosion of misinformation that has served as an increasing obstacle to effective patient care within health systems. When patients are misled about medical conditions or treatments, the potential for conflict increases, while the respect for medical professionals decreases. In such situations, the propensity for affective violence within hospitals increases. But a newer driver — social media — can reveal medical and nursing providers' personal information to those intent on committing targeted violence. During the COVID-19 pandemic, we saw that social media contributed to dramatic increases in interpersonal violence, risk-taking behavior and dysfunctional interpersonal dynamics.[36]

Just as teachers do not enter their field in order to focus on and prevent targeted violence, medical and nursing personnel do not enter the field in order to prioritize threat assessment and management of potential perpetrators. However, no matter the field, professionals are unprepared unless and until they receive sufficient awareness and training that influences new proactive behaviors.

---

35 The School Shooter: A Threat Assessment Perspective, U.S. Department of Justice, Federal Bureau of Investigation, Critical Incident Response Group, National Center for the Analysis of Violent Crime, 1999.

36 Abdallah HO, Zhao C, Kaufman E, et al: Increased firearm injury during the COVID-19 pandemic: A hidden urban burden. *J Am Coll Surg* 2021; 232:159–168.e3

In the fast-paced culture of health care, with its accelerated patient and staff turnover, health care systems across the country face extraordinary challenges in the areas of threat assessment and management. There is a dearth of options for individuals with serious mental illness who threaten violence and require commitment and treatment. It is ironic that, although our complex threat environment demands more solutions, patients' families face decreasing options for hospitalizing and treating those who threaten violence due to severe mental illness. Consequently, emergency departments across the country have had to adapt their own environments in order to meet the unique needs of these severely ill patients who may present a significant threat. In response to these new imperatives, forensic assertive community treatment programs have been developed.[37] In concert with our judicial system, these patients are provided a means to dramatically increase compliance with medications that allow for functioning in the community — but these programs are not effective without awareness and/or adequate funding.

The need to protect health care workers has been recognized at the legislative level.[38] Hospitals by nature are soft targets in that they are designed to serve the public's health and welfare and be accessible and welcoming to the public at large. To safeguard these facilities is a challenge even greater than protecting schools, which have a much more defined and expected group of individuals who receive services. To meet this challenge, it is essential that the federal government provides behavioral analysis resources in collaboration with federal, state and local law enforcement, as well as stakeholders in the health care system.

What we have learned about targeted violence is that when it is carried out, the consequences of death and injury are enormous and shake the foundations of trust necessary between the public and hospitals. Less recognized is the cascade of morbidity due to the psychological trauma that can profoundly impact health care professionals, patients and their families. To be successful, this expertise must arise not only from current best practices exercised by leading hospitals but also through collaborative partnerships with stakeholders across the health care, law enforcement and legislative domains.

37 Lamberti, JS, Weisman, RL, Essential Elements of Forensic Assertive Community Treatment, *Harvard Review of Psychiatry*, Volume 29 • Number 4 • July/August 2021

38 Hospital Employee Health; Feb 2024, Vol. 43 Issue 2, p1-12, 12p

Vulnerabilities in the Patient Care Cycle: Utilizing a Proactive Approach in Mitigating Affective Violence

Nicole Tuomi Jones, Ph.D.
Licensed Psychologist with the Behavioral Threat Assessment Unit
North Carolina State Bureau of Criminal Investigation

A patient is admitted to the emergency department (ED) to receive treatment under an involuntary commitment. He must stay in the ED until a bed becomes available in a psychiatric facility. While in the ED, he paces in front of the nursing station, makes inappropriate sexual comments to staff and other patients, and refuses to take the medication prescribed. Nursing staff reports he has been loud and threatening since he arrived and yells obscenities when approached for vitals. Is he an actual threat, or is he just blustering? Does his behavior rise to the level of reporting? How should staff report and document the behavior? Are there strategies that hospital staff can use to de-escalate the situation? Should security forces be called, or would a specialist in behavioral health be better? Above all, are the health care workers and the patients they care for safe?

The prevalence of hospital-based violence is not an emerging issue. In 1996, the Occupational Safety and Health Administration (OSHA) issued its first guidelines for workplace violence prevention for health care workers. Despite these guidelines, injuries from workplace violence in health care settings have increased almost every year since 2011, despite efforts to address the issue via violence prevention education programs with inconclusive evidence of effectiveness.[39,40] In 2020, 3 out of every 4 nonfatal workplace violence injuries involved health care workers, making health care facilities one of the most dangerous places to work in the United States. A 2022 umbrella review of meta-analyses found the overall prevalence of health care workplace violence was 58.7%, with the largest contributor being verbal.[41]

Affective Violence

OSHA defines workplace violence as "any act or threat of physical violence, harassment, intimidation, or other threatening disruptive behavior that occurs at the work site."[42] Impromptu, affective violence (AV) at the point of care, perpetrated by a patient the hospital serves, remains the largest category of violence experienced by health care staff.[43] This type of violence is unplanned and is driven by negative emotions experienced by the person in the moment (e.g., anger, sadness, frustration, fear, disappointment, boredom) that move quickly from a grievance to a verbal or physical attack.[44]

Vulnerabilities Associated With Increased AV Risk

AV is the result of an interaction between a person and their environment. The reasons patients engage in AV vary, and there are typically multiple drivers that result in AV directed at health care workers. Individual differences (e.g., genetics, impulse control, life experiences) contribute to who will become aggressive under varying sets of conditions.[45,46]

---

39 Occupational Safety and Health Administration (OSHA) (n.d.). Guidelines for Preventing Workplace Violence for Healthcare and Social Service Workers, Retrieved from: https://www.osha.gov/sites/default/files/publications/osha3148.pdf.

40 Provost, S., MacPhee, M., Daniels, M.A., Naimi, M., & McLeod, C. (2021). A realist review of violence prevention education in healthcare. *Healthcare (Basel)*, 9, 339.

41 The Joint Commission implemented new, proactive workplace violence prevention standards for hospitals on January 1, 2022, and for behavioral health care facilities on July 1, 2024.

42 Occupational Safety and Health Administration (OSHA) (n.d., b). Workplace violence, Retrieved from: https://www.osha.gov/workplace-violence .

43 ECRI (2017, May 24). Violence in healthcare facilities. Healthcare Risk Control. Retrieved from: https://www.ecri.org/components/HRC/Pages/SafSec3.aspx.

44 Calhoun, F.S. & Weston, S.W. (2016). Threat assessment and management strategies: Identifying the howlers and hunters (2nd ed.). CRC Press Taylor and Francis Group.

45 Tuvblad C, & Baker LA. (2011). Human aggression across the lifespan: genetic propensities and environmental moderators. *Advanced Genetics*, 75, 171-214. doi: 10.1016/B978-0-12-380858-5.00007-1.

46 Wang, L., Li, T., Gu, R., & Feng, C. (2024). Large-scale meta-analyses and network analyses of neural substrates underlying human escalated aggression, *NeuroImage*, 299, 120824. https://doi.org/10.1016/j.neuroimage.2024.120824.

Environmental factors that have been found to increase the risk of AV include the physical features of the facility (e.g., poor lighting or environmental design, hospital location); inadequate security (e.g., unrestricted public access, presence of firearms, inadequate security personnel); staffing issues (e.g., understaffing, high turnover, working alone or moving patients); and hospital policy and procedures (e.g., lack of means of emergency communication, lack of training and policies for staff, the perception that violence is tolerated and reporting will have no impact). Other dynamic environmental conditions that increase risk include long wait times between staff and patient interactions, as well as rising patient expectations related to access, timeliness and efficacy of care.[47,48,49]

There also are multiple patient vulnerabilities that increase the likelihood of AV. A systematic review of studies in inpatient behavioral health care settings identified dynamic risk factors associated with increased physical violence risk in two or more studies. These included mental health risk factors (having an affective disorder, having anxiety, poor mental well-being), behavioral risk factors (antisocial behavior, hostility, impulsivity, boisterousness, confusion, easily angered when requests are denied, negative attitudes, unwilling to follow directions, problems with rule adherence, verbal threats), and functional risk factors (lack of insight, poor personal hygiene, problematic coping skills).[50] In non-behavioral hospitals, several additional dynamic patient risk factors have been found to increase AV risk, including intoxication, cognitive changes,[49] physical pain, transient stressors, prior trauma experiences, problems with emotional regulation, maladaptive coping responses, interpersonal chaos and poor overall functioning.[48] The past few years have also seen attitudes or beliefs about COVID-19 as a contributor to violence and mistreatment of staff by patients and visitors.[51]

Dynamic risk factors have been shown to share a closer temporal relationship to aggressive behaviors in behavioral health care settings than static risk factors.[51] When adverse environmental conditions are combined with these individual risk factors, the risk for AV increases. Hospital staff must feel confident in communicating with and providing care for patients in these high-risk situations.[52]

The Need for Assessment

Data on the exact rates of AV varies due to differences in the way researchers operationally define violent behavior, how behavior is measured, and a lack of systematic or structured documentation of these behaviors.[49] For example, does the patient in the scenario above meet the definition of "workplace violence?" If so, how should this behavior be documented? What policies and procedures are in place to address threatening and disruptive behaviors that may occur prior to a serious physical attack? If hospitals desire to address workplace violence, they must first implement evidence-based assessment tools in an ongoing and sustainable manner to track the rate of disruptive, threatening and aggressive behaviors.[53] Effective intervention requires understanding the scope of the problem and the ability to conduct an annual worksite analysis of any violence reduction efforts. There are existing tools to record the frequency and magnitude of aggressive behaviors for use in hospital settings, and research has found they can be implemented

---

47 Nowrouzi-Kia, B., Chai, E., Usuba, K., Nowrouzi-Kia, B., & Casole, J. (2019). Prevalence of type II and type III workplace violence against physicians: A systematic review and meta-analysis. *Occupational and Environmental Medicine*, 10, 99-110.

48 O'Brien, C.J., van Zundert, A.A.J., & Barach, P.R. (2024). The growing burden of workplace violence against healthcare workers: trends in prevalence, risk factors, consequences, and prevention– a narrative review. *The Lancet*, 72, 1-16.

49 Occupational Safety and Health Administration (OSHA) (2015). Workplace violence in healthcare: Understanding the challenge. Retrieved from: https://www.osha.gov/sites/default/files/OSHA3826.pdf.

50 Greer, B., Taylor, R.W., Cella, M., Stott, R., & Wykes, T. (2020). The contribution of dynamic risk factors in predicting aggression: A systematic review including inpatient forensic and non-forensic mental health services. *Aggression and Violent Behavior*, 53, 101433. https://doi.org/10.1016/j.avb.2020.101433.

51 Meese, K.A., Boitet, L.M., Schmidt, J.J., Borkowski, N., Sweeney, K.L. (2024). Exploring national trends and organizational predictors of violence and mistreatment from patients and visitors. *Journal of Healthcare Management, 69,* 29-44. DOI: 10.1097/JHM-D-23-00105.

52 Lim, M.C., Jeffree, M.S., Saupin, S.S., Giloi, N. & Lukman, K.A. (2022). Workplace violence in healthcare settings: The risk factors, implications and collaborative preventive measures. *Annals of Medicine and Surgery*, 78. doi: 10.1016/j.amsu.2022.103727.

53 Arnetz, J.E., Hamblin, L., Russell, J., Upfal, M.J., Luborsky, M., Janisse, J., & Essenmacher, L. (2017). Preventing patient-to-worker violence in hospitals: Outcome of a randomized controlled intervention. *Journal of Occupational and Environmental Medicine*, 59, (18-27).

into routine documentation procedures while still meeting regulatory requirements.[54,55,56,57]

Leadership's Commitment to Safety

Just because AV emerges quickly does not mean AV cannot be prevented or the impacts reduced if it occurs.[48] Violence prevention programs that include the components outlined in the new Joint Commission standards (2021, 2023) have been found to decrease the rate of violence against nurses.[58] Hospitals must first commit to improving the culture of safety from all position levels in an organization and address environmental issues that are within reach (e.g., staffing levels, improved security measures). Next, hospitals must implement robust standard operating procedures to deal with the continuum of aggressive behaviors (prevention to de-escalation to crisis response) discussed below. Finally, violent incidents should be addressed in an urgent and timely way by hospital administration, and there should be a formal process that establishes a clear line of accountability for implementing an immediate plan of protection for patients and staff when a crisis occurs.

Violence Prevention Programs

To maximize health care facilities' limited budgets and minimize extra demands on staff time, it is essential that hospital management teams implement the most effective, proactive violence prevention programs. Here are three interventions that should be included in every hospital violence prevention program:

Increase the frequency of interactions between hospital staff and patients. Situations that make patients and their families feel unimportant (e.g., lack of information or communication, long wait times, lack of access to health care personnel) can trigger feelings of frustration and anger. Research has shown that in behavioral health hospitals, increased interaction with staff is associated with better patient outcomes, regardless of the social environment.[59] Too often, patients who engage in disruptive behavior get the attention of hospital staff. This reinforces the disruptive behavior not only for the patient but also for other patients and families who may be watching. Effective, proactive communication delivered in a timely and consistent way can help prevent increased emotional arousal that results in problematic interactions, including AV.[60,61] This engagement been identified as a key component of hospital safety, and models for the communication skills needed for these interactions have been developed.[62,63,64] However, these interactions do not have to be provided by a doctor or a nurse; they can be provided by administrative personnel, mental health professionals (e.g., social workers) or line-level nursing staff (e.g., certified nursing assistants) who have received training on effective communication. Practical guidelines regarding the purpose, timing, content and number of interactions can be developed by hospital administration and nursing managers

---

54 Jones, N.T., Sheitman, B., Hazelrigg, M., Carmel, H., Williams, J., & Paesler, B. (2007). Development of a clinical instrument to record sexual aggression in an inpatient psychiatric setting. *Journal of Sexual Aggression*, 13, 51-58.

55 Mistler, L.A. & Friedman, M.J. (2021). Instruments for measuring violence on acute inpatient psychiatric units: Review and recommendations. *Psychiatric Services*, 73, 650-657. doi: 10.1176/appi.ps.202000297.

56 Ramesh, T., Igoumenoub, A. , Vazquez Montesc , M., & Fazel, S. (2018). Use of risk assessment instruments to predict violence in forensic psychiatric hospitals: a systematic review and meta-analysis. *European Psychiatry*, 52, 47–53. http://dx.doi.org/10.1016/j.eurpsy.2018.02.007

57 McGill, A.C., Jones, N.T., Boss, A.R. & Sheitman, B. (2017). Enhancing evidence-based clinical assessment in a large, public psychiatric hospital: Using behavior data collected by direct care nursing staff. *Worldviews on Evidence-Based Nursing*, 14, 256-248.

58 Somani, R., Muntaner, C., Hillan, E., Velonis, AJ, & Smith, P. (2021). A systematic review: Effectiveness of interventions to de-escalate workplace violence against nurses in healthcare settings. *Safety and Health at Work*, 12, 289-295.

59 Coleman, J.C., Paul, G.L., & Schatschneider, C.W. (2007). Impact of staff attention on predicting post-discharge community tenure of psychiatric inpatients. *Psychological Services*, 4, 306-315.

60 King, A. & Hoppe, R.B. (2013). Best practice for patient-centered communication: A narrative review. *Journal of Graduate Medical Education*, September 2013, 5, 385–393, doi: http://dx.doi.org/10.4300/JGME-D-13-00072.1 .

61 Linehan, M.M. (1993). Cognitive-behavioral treatment of borderline personality disorder. Guilford Press: NY.

62 American Psychiatric Nurses Association (2024). Patient engagement toolkit. Retrieved from: https://www.apna.org/resources/apna-patient-engagement-toolkit/.

63 Delaney, K.R., Shattell, M., & Johnson, M.E. (2017). Capturing the interpersonal process of psychiatric nurses: A model for engagement. *Archives of Psychiatric Nursing*, 31, 634-640.

64 McAllister, S., Robert, G, Tsianakas, V., & McCrae, N. (2019) Conceptualizing nurse-patient therapeutic engagement on acute mental health wards: An integrative review. *International Journal of Nursing Studies*, 93, 106-118. doi: 10.1016/j.ijnurstu.2019.02.013.

Train staff on effective communication in adverse interactions. In addition to environmental risks, direct care staff are required to engage in difficult interactions with patients that place them at greater risk to be a victim of AV. Hospital staff must be educated on how to communicate effectively in interactions known to be potentially problematic and therefore at a possibly increased risk for AV (e.g., patient transport, procedures the patient does not want to receive or engage in, setting limits on disruptive and aggressive patient behavior, saying no to a patient's request).[65] Staff must be trained to identify the signs of escalating behavior, such as psychomotor agitation, increased rate or volume of speech, and affective or facial changes. Next, staff must be taught how to apply specific verbal techniques that reduce the emotional arousal that leads to AV.[66] Training should include practice performance under stressful and real-world situations to a competency standard, so staff know what to do when they are confronted with anxious, hostile or threatening behavior. [67,68,69]

Practice violence response protocols. By the time a physical assault has begun, prevention strategies have failed. Nonetheless, robust policies and procedures can improve response times and minimize unwanted negative outcomes (e.g., restraint use, injury, death). Violence response protocols should be initiated when a patient poses an imminent risk of inflicting serious physical harm or death on themselves or others.[65] Hospital staff should be trained in self-defense maneuvers, as well as when and how to notify behavioral response teams or hospital security in crisis situations. Multidisciplinary behavioral response teams trained in therapeutic crisis intervention have been found to reduce unwanted negative outcomes (e.g., security calls, restraint use, staff injuries)and are the emerging standard of care in providing ethical interventions for behavioral health emergencies.[70,71,72]

Conclusion

There is mounting pressure on health care workers to not only provide excellent, evidence-based medical care but also to deal with the increasing rates of violence and threats of violence in the workplace setting. This contributes to poor worker outcomes (e.g., absenteeism, staff turnover, workplace stress and burnout) *and* poor patient outcomes (e.g., reduced patient safety and medical errors).[48] To achieve the goal of improving hospital safety, hospital risk management departments must be provided with the necessary resources to design, implement and monitor violence prevention efforts.

---

65 Taylor, J.L., & Rew, L. (2011). A systematic review of the literature: Workplace violence in the emergency department. *Journal of Clinical Nursing*, 20, 1072-1085. doi:10.1111/j.1365-2702.2010.03342.x

66 Stensrud, T.L., Gulbrandsen, P., Mjaaland, T.A., Skretting, S., & Finset, A. (2014). Improving communication in general practice when mental health issues appear: Piloting a set of six evidence-based skills. *Patient Education and Counseling*, 95, 69-75.

67 Epstein, R.M. & Hundert, E. (2002). Defining and assessing professional competence. *Journal of the American Medical Association*, 287, 226-235. doi:10.1001/jama.287.2.226

68 Jones, N.T., Menditto, A.A., Geeson, L.R., Larson, E. & Sadewhite, L. (2001). Teaching social-learning procedures to paraprofessionals working with individuals with severe mental illness in a maximum-security forensic hospital. *Behavioral Interventions*. 16, 167-179. DOI: 10.1002/bin.090.

69 Holloman, G.H. Jr & Zeller, S.L. (2012). Overview of Project BETA: Best practices in Evaluation and Treatment of Agitation. *Western Journal of Emergency Medicine*,13, 1-2. doi:

70 Choi, K.R., Omery, A.K., & Watkins, A.M. (2019). An integrative literature review of psychiatric rapid response teams and their implementation for de-escalating behavioral crises in nonpsychiatric hospital settings. *The Journal of Nursing Administratio*n, 49, doi: 10.1097/NNA. 0000000000000756.

71 Godfrey, J.L., McGill, A. C., Jones, N.T., Oxley, S.L., Carr, R.M. (2014). Anatomy of a transformation: A systematic effort to reduce mechanical restraints at a state psychiatric hospital. *Psychiatric Services*, 65, 1277-1280.

72 Parker, C.B., Calhoun, A., Wong, A.H., Davidson L., & Dike, C. (2020). A call for behavioral emergency response teams in inpatient hospital settings. *American Medical Association Journal of Ethics, 22, 956-964. doi:10.1001/amajethics.*2020.956.

The Pathway to Targeted Violence: Predatory Behavior, Shame and the Thin Line Between Suicide and Homicide

Supervisory Special Agent Melissa R. Stormer, Psy.D.
Air Force Office of Special Investigations
Task Force Officer, FBI BAU-1

Understanding and mitigating predatory violence requires an integrated approach that considers the behavioral pathway to violence, emotional drivers like shame and the complex interplay between suicidal and homicidal tendencies. These dynamics are of particular importance in hospital settings where both affective and predatory violence may occur.

Violence can be broadly categorized as affective or predatory. Affective violence, driven by immediate emotions such as anger or fear, is impulsive and reactive. It often arises in stressful scenarios where emotions run high, such as emergency departments. Predatory violence, on the other hand, is premeditated and goal-oriented.[73,74] Targeted violence, including mass shootings or revenge attacks, falls into this category. Predatory violence is methodical, involving calculated actions that align with specific objectives, such as achieving retribution or recognition. While these forms of violence are distinct, overlap can occur. For example, an individual's initial affective outburst may lead to rumination and escalate into a planned act of retaliation. Understanding these distinctions is crucial for health care professionals to tailor their interventions effectively.

Health care settings, often viewed as places of healing, are not immune to targeted violence. Research highlights the prevalence of grievances in health care-related attacks, often stemming from dissatisfaction with care or perceived mistreatment.[75] Recognizing early indicators such as fixation on grievances, leakage of intent and unusual preparations is essential for proactive threat assessment.[76,77,78] Health care professionals must be vigilant in identifying these warning signs and collaborating with threat assessment teams to address potential risks. De-escalation techniques are effective for addressing affective violence, while predatory violence requires robust threat assessment and long-term management strategies.[79,80] Training and collaboration across departments can help identify and address potential risks before they escalate.

Understanding the pathway to targeted violence is crucial for hospitals aiming to mitigate risks and enhance safety. The pathway model consists of distinct stages — grievance, ideation, research and planning, preparation, and breach — that collectively describe how an individual progresses toward committing an act of targeted violence.[81] While the pathway is often sequential, it is not strictly linear; individuals can pause, exit or re-enter the pathway.

---

73 Meloy, J. R. (2006). Affective and predatory violence: A bimodal classification system of human aggression. *Aggression and Violent Behavior*, 11(1), 1–15. https://doi.org/10.1016/j.avb.2005.05.002

74 Amman, M., Bowlin, M., Buckles, L., Burton, K. C., Brunell, K. F., Gibson, K. A., Griffin, S. H., Kennedy, K., & Robins, C. J. (2017). Making prevention a reality: Identifying, assessing, and managing the threat of targeted attacks. U.S. Department of Justice, Federal Bureau of Investigation.

75 Thomas, S. P., & Pollio, H. R. (2002). Violence in a place of healing: Addressing aggression in healthcare settings. *Journal of Nursing Scholarship*, 34(4), 389–395. https://doi.org/10.1111/j.1547-5069.2002.00389.

76 Amman, M., et al. Making prevention a reality.

77 Meloy, J. R., Hoffmann, J., Roshdi, K., & Guldimann, A. (2014). Are all pathway behaviors observable? A study of targeted violence in German public schools. *Journal of Threat Assessment and Management*, 1(4), 243–255. https://doi.org/10.1037/tam0000022

78 Almond, L., O'Neill, L., & Smith, R. (2024). Differentiating between harmless and harmful threats: An examination of behavioral indicators in threat assessment. *Journal of Behavioral Threat Assessment and Management*.

79 Meloy, J.R. Affective and predatory violence.

80 Almond, L., et al. Differentiating between harmless and harmful threats.

81 Amman, M., et al. Making prevention a reality.

Stages of the Pathway

1. **Grievance.** The process begins with a perceived grievance. This is typically a deeply felt sense of injustice or humiliation that creates emotional turmoil. For example, in hospital settings, a patient or family member might harbor resentment due to an adverse medical outcome, miscommunication or dissatisfaction with care. It is important to note that this injustice or humiliation is perceived, meaning it is not necessarily based in reality. The grievance can fester, particularly in environments where emotional regulation is challenged by stress or personal loss. This stage is foundational, as unresolved grievances can evolve into fixations on retribution or justice.[82]
2. **Ideation.** During this phase, the individual begins to entertain the possibility of violence as a solution to their grievance.[83] This ideation often includes fantasies of retaliation or achieving notoriety. In a medical context, such ideation might target specific staff members or facilities perceived as responsible for the grievance. The progression from grievance to ideation underscores the importance of early intervention and support systems.
3. **Research and Planning.** Here, the individual collects information, such as identifying potential targets, researching past attacks or attackers, understanding security protocols, or acquiring necessary tools.[84,85] This stage is marked by methodical preparation and may comingle with other steps. Hospitals, which are open and accessible environments, may be particularly vulnerable during this phase due to the availability of public information about facility layouts and schedules.
4. **Preparation.** Preparation involves tangible steps toward committing the act, such as obtaining weapons or rehearsing the attack, engaging in end-of-life planning (e.g., giving away belongings), or creation of artifacts meant to be left behind.[86] This stage is where the person of concern moves from thought to action, and this readiness to act signals a significant escalation in the threat level. For individuals with prior training or resources, such as former military personnel, this stage may be abbreviated or skipped entirely.
5. **Breach.** This final step involves bypassing or circumventing security measures or boundaries at the intended target location.[87] Such activities might include rehearsing actions, stalking the target or testing the effectiveness of security protocols. Additionally, the Behavioral Analysis Unit (BAU) has broadened this concept to include cyber intrusions aimed at uncovering security vulnerabilities, accessing protected information, or otherwise advancing an attack plan through unauthorized system access. Breach behaviors may take place immediately before an attack or at earlier stages of preparation, depending on the perpetrator's intent and planning. Like with other steps, it is important to consider native knowledge, as this step may not always be necessary. For example, a person familiar with the hospital's layout and security (e.g., a former employee) may not need to conduct a breach prior to an attack.

Beyond the pathway, attackers often exhibit specific warning behaviors that signal escalating risk, including novel aggression, identification, fixation and leakage.[88] **Novel aggression** refers to acts of violence or hostility that are uncharacteristic for the individual and indicate a significant shift in behavior, such as a previously nonviolent person engaging in verbal threats or physical confrontations. **Identification** occurs when an individual adopts elements associated with prior attackers, such as mimicking their appearance, dressing in pseudo-commando clothing or glorifying individuals responsible for similar violent acts. This behavior reflects a growing connection to violent ideologies or personas. **Fixation** is marked by an increasing preoccupation with a specific person, cause or grievance. It often involves persistent focus, increasingly rigid opinions and negative characterizations of the target, coupled

---

82 Ibid.

83 Meloy, J. R., Hoffmann, J., Roshdi, K., & Guldimann, A. (2014). Are all pathway behaviors observable? A study of targeted violence in German public schools. *Journal of Threat Assessment and Management*, 1(4), 243–255. https://doi.org/10.1037/tam0000022

84 Amman, M., et al. Making prevention a reality.

85 Almond, L., et al. Differentiating between harmless and harmful threats.

86 Amman, M., Bowlin, M., Buckles, L., Burton, K. C., Brunell, K. F., Gibson, K. A., Griffin, S. H., Kennedy, K., & Robins, C. J. (2017). Making prevention a reality: Identifying, assessing, and managing the threat of targeted attacks. U.S. Department of Justice, Federal Bureau of Investigation.

87 Ibid.

88 Ibid.

with an angry emotional undertone. Finally, **leakage** refers to the intentional or unintentional sharing of information about an impending violent act.[89, 90] This may manifest through verbal statements, online posts or actions that reveal the individual's plans or intentions. Leakage is especially critical in threat assessment, as it provides an opportunity for intervention before further escalation occurs. In health care settings, recognizing leakage — such as a patient or family member expressing violent fantasies or grievances — can enable proactive measures to address and mitigate potential threats. By training staff to identify and report such indicators, hospitals can play a pivotal role in preventing acts of targeted violence.

Shame as a Catalyst for Violence

Shame, as conceptualized in "Shame, Guilt, and Violence" by James Gilligan, M.D., James is a profound and destabilizing emotion that arises when an individual perceives a loss of respect, dignity or status in the eyes of others or themselves.[91] It is an acute internal experience of feeling diminished, exposed or humiliated, often tied to a sense of unworthiness or failure. Shame is a global analysis of the self and differs from guilt, which centers on a particular action or decision. An individual experiencing guilt typically acknowledges that they did something wrong but still may see themselves as a fundamentally good person. This distinction is critical, as guilt is often associated with empathy, remorse and a desire to make amends. Individuals experiencing guilt are more likely to take responsibility for their behavior and engage in reparative actions, such as apologizing or changing their behavior in the future.

According to Gilligan, shame becomes particularly dangerous when it threatens the viability of the self and cannot be resolved or alleviated through nonviolent means. This unresolved shame can fuel a desperate need to restore self-esteem or control, often through externalized aggression or violence, especially when combined with societal pressures such as rigid gender roles or cultural norms that equate violence with honor and masculinity. Understanding the mechanisms of shame and its connection to violence is essential for identifying and mitigating risks in environments where interpersonal conflicts and grievances frequently arise, such as hospitals. In the context of predatory violence, shame often fuels the planning and execution of calculated attacks as perpetrators seek to externalize their pain and reclaim control. According to Gilligan's research, there are four preconditions under which shame is most likely to lead to violence:

1. **Absence of Guilt or Remorse.** The individual has not yet developed the capacity for guilt and remorse, or situational factors have diminished these feelings. Without these internal checks, the likelihood of engaging in violent behavior increases. This can occur due to developmental delays, personality disorders or environmental influences that neutralize guilt, allowing shame to dominate the individual's emotional response.
2. **Overwhelming Shame.** The intensity of shame and humiliation experienced is so severe that it threatens the cohesion and viability of the self, metaphorically or literally creating a "death of the self." In such cases, the individual may perceive violence as the only way to restore their sense of identity or self-worth. This is particularly relevant in hospital settings, where patients or families may feel powerless and demeaned by the health care process.
3. **Lack of Nonviolent Solutions.** The individual perceives themselves as having no nonviolent means to save or restore their self-esteem. This perception drives the individual to consider violence as a last resort, particularly when they believe other methods have failed or are inaccessible. For example, unresolved grievances against health care providers might intensify if the individual feels their concerns are ignored.
4. **Gender Role Pressures.** For men in patriarchal cultures, socialization into rigid gender roles may teach them that violence is necessary to maintain their masculinity. Nonviolence in such scenarios is shamed, leading to feelings of emasculation or inadequacy. This precondition can exacerbate the shame-violence connection, especially in environments where male identity is closely tied to control and dominance.

---

89 Ibid.

90 Meloy, J.R., O'Toole, M.E. (2011). The concept of leakage in threat assessment. *Behavioral Sciences & the Law*, 29(4), 513–527. https://doi.org/10.1002/bsl.986

91 Gilligan, J. (2003). Shame, guilt, and violence. *Social Research: An International Quarterly*, 70(4), 1149–1180.

These preconditions create a fertile emotional and cognitive environment for grievances to fester and escalate, particularly if the individual already feels disempowered or humiliated. Gilligan emphasizes that unresolved shame often leads to externalization, where the individual redirects their internal pain outward through violence.[92] This is especially evident in predatory violence, where perpetrators frame their actions as justified retribution against those they believe are responsible for their suffering. By identifying these preconditions early, health care professionals can intervene to prevent grievances from escalating to violence. Proactive communication, validation of concerns and pathways for conflict resolution are essential tools for reducing the impact of shame in hospital settings.

The Thin Line Between Suicide and Homicide

Targeted violence frequently intertwines with suicidal intent. The interpersonal theory of suicide posited by Thomas Joiner, Ph.D., identifies three key components that elevate suicide risk: thwarted belongingness, perceived burdensomeness and acquired capability for self-harm.[93] Thwarted belongingness reflects a profound sense of social disconnection, while perceived burdensomeness involves the belief that one's existence imposes an undue burden on others. Acquired capability, often developed through exposure to pain or violence, reduces the fear of death, enabling individuals to act on suicidal impulses.

When these elements converge with externalized grievances, the line between suicide and homicide becomes perilously thin. Joiner's concept of "suicide-murder" is particularly relevant to mass casualty events, including active shooter incidents. He posits that perpetrators often decide to die but deem it unjust that they should die alone while others live.[94] This sense of "unfairness" drives the lethal blending of suicide and homicide, which is often framed as a distorted form of justice or retribution. In the context of shame and the thin line between suicide and homicide, targeted attacks often reflect the offender's internal conflict.[95,96] For instance, feelings of humiliation or ostracism may manifest as both self-directed despair and outward resentment and aggression. Hospitals, as places of healing, must remain vigilant to such dual risks, as unresolved shame or perceived grievances can culminate into catastrophic outcomes.

Questions to Consider When Assessing Suicidal and/or Homicidal Intent

When assessing suicidal ideation or intent, it is essential to prioritize open-ended questions to encourage the individual to share their thoughts and feelings in greater detail. While yes/no questions can provide initial insight, following up with open-ended prompts such as, "Can you describe that?" or "Tell me more about ..." helps to gather more comprehensive information. These conversations can be challenging, so it is often helpful to begin by identifying the situation and associated emotions the individual may be experiencing (e.g., overwhelmed, hopeless, helpless, lonely, angry, or ashamed) and explore from there. By creating a safe and empathetic environment, health care professionals can facilitate meaningful dialogue and gain a deeper understanding of the patient's emotional state and potential risk factors.

Please note: The questions below are not meant to replace existing measures, but rather to explore other questions that could be considered to provide additional context.

Assessing for Suicidal Ideation

- **Exploring emotional distress and thoughts of self-harm:**
  - Tell me how you've been feeling recently.
  - Tell me about your typical day (assessing for isolation).
  - What thoughts have been going through your mind when you feel the most stressed/hopeless/angry?

92 Ibid.

93 Van Orden, K. A., Witte, T. K., Cukrowicz, K. C., Braithwaite, S. R., Selby, E. A., & Joiner, T. E. (2010). The interpersonal theory of suicide. *Psychological Review*, 117(2), 575–600. https://doi.org/10.1037/a0018697

94 Joiner, T. (2013). *The perversion of virtue: Understanding murder-suicide*. Oxford University Press.

95 Gilligan, J. Shame, guilt, and violence.

96 Joiner, T. The perversion of virtue.

- Have there been times when you've felt like you didn't want to live anymore? Tell me more.
- Tell me about when you are in your deepest, darkest spot. What thoughts do you have when you are feeling hopeless?
- Tell me about the fantasies you have about dying.
- Tell me how you have rehearsed ending your life.
- Who would you want to find you? Why?

- **Understanding coping and protective factors:**
  - What helps you cope when you feel ____?
  - Who in your life do you feel most connected to or supported by?
  - What are some things that keep you going, even during tough times?
  - What prevents you from hurting yourself?

- **Exploring plans or intent:**
  - When you are feeling ____, what actions do you consider taking?
  - When you've had thoughts about not wanting to live, have you thought about how you might act on those feelings?
  - Have you made any plans to hurt yourself or take your life? What do those plans look like?
  - Have you thought about when or where you might act on these feelings?

Assessing for Homicidal Ideation

- **Exploring anger and interpersonal conflict:**
  - Have you been feeling angry or frustrated with anyone recently? How have you been handling those feelings?
  - Are there situations or people in your life that have been causing you significant stress or conflict? Tell me more.
  - Have you ever thought about harming someone because of how they've treated you or made you feel? Tell me more.

- **Assessing grievance and justification:**
  - Have you ever felt that someone has wronged you in a way that you couldn't let go of? Tell me more.
  - How often do you think about_____? (assessing for rumination/fixation)
  - What people or situations in your life do you feel are unfair or unbearable to deal with?
  - What kinds of thoughts or solutions have crossed your mind when thinking about those conflicts?
  - Who is not listening to you? Tell me more.
  - Who has caused you pain and suffering? Tell me more.
  - Is there someone who needs to suffer like you are suffering? Tell me more.
  - Tell me what other alternatives are available for resolving your grievance peacefully.

- **Exploring plans or intent:**
  - When you think about (person/situation/grievance), what actions do you consider taking?
  - Do you ever fantasize about getting revenge about (situation/grievance)? Can you share those thoughts with me?
  - Do others need to pay for what has happened to you? Tell me more.
  - Have you had thoughts about harming someone else? What have those thoughts been like?
  - Have you thought about how, when or where you might act on those feelings?
  - How would you carry out those thoughts if you wanted to?
  - Do you have access to weapons to carry out your plan? If your weapons are secured, tell me how they are secured and who has access.

- **Follow-up and building rapport:**
  - I really appreciate you sharing this with me. Tell me more about what's been weighing on your mind.
  - It's brave to talk about these difficult feelings. How can I best support you right now?
  - Is there someone I can call or bring into the conversation that would be helpful going forward?
  - Have you ever felt like these thoughts might get out of control? What can we do together to make sure you stay safe?
  - What makes these thoughts better or less strong?

Conclusion

Targeted violence rarely occurs without warning. Understanding the critical factors that drive individuals from ideation to action is essential for effective prevention and intervention. When a person of concern progresses from thought to action in targeted violence, four key factors are typically present: 1) they feel their act of violence is justified; 2) they believe there are no alternatives to achieve their goals; 3) they are willing to accept the consequences of their actions (i.e., death or prison); and 4) they possess the ability to carry out the act. These factors highlight the importance of recognizing behavioral indicators and addressing grievances before they escalate. Understanding the pathway to violence, the role of shame and the interplay between suicide and homicide is essential for preventing targeted violence in hospital settings. By recognizing the early stages of the pathway, addressing unresolved grievances and implementing robust behavioral threat assessment and management protocols, hospitals can proactively disrupt the progression toward violence.

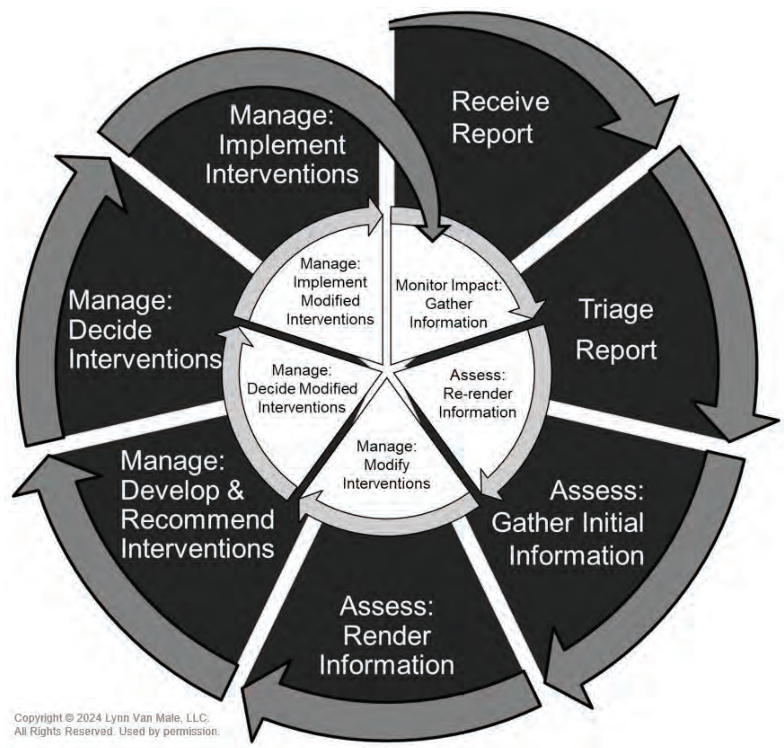
The Importance of Behavioral Threat Assessment and Management for Hospitals and Health Systems

Lynn Van Male, Ph.D.
Senior Director, Threat Management
National Security Services, Kaiser Permanente
Assistant Clinical Professor of Psychology, Oregon Health and Science University

What Is Behavioral Threat Assessment and Threat Management?

Behavioral threat assessment and management (BTAM) is an ongoing and iterative process — not a linear outcome. Examined in its component parts, threat assessment is a "systematic, fact-based method of investigation and examination that blends the collection and analysis of multiple sources of information with published research and practitioner experience, focusing on an individual's patterns of thinking and behavior to determine whether, and to what extent, a person of concern is moving toward an attack."[97] Threat management is the act of "managing a person of concern's behavior through interventions and strategies designed to disrupt or prevent an act of targeted violence."[98] The multidisciplinary BTAM process itself is well defined.[99,100] Although slight semantic variation exists across models, the BTAM process aims to identify at the earliest possible moment that an individual is progressing toward an act of violence and implement interventions that disrupt that progression (see Figure 1).

Figure 1. Ongoing and Iterative BTAM Process



97 Amman, M., Bowlin, M., Buckles, L., Burton, K. C., Brunell, K. F., Gibson, K. A., Griffin, S. H., Kennedy, K., & Robins, C. J. (2017). Making prevention a reality: Identifying, assessing, and managing the threat of targeted attacks. U.S. Department of Justice, Federal Bureau of Investigation.

98 Meloy, J. R., Hoffmann, J., Guldimann, A., & James, D. (2012). The role of warning behaviors in threat assessment: An exploration and suggested typology. *Behavioral Sciences & the Law*, 30(3), 256-279.

99 Amman, M., et al. Making prevention a reality.

100 National Threat Assessment Center. (2024). Behavioral Threat Assessment Units: A Guide for State and Local Law Enforcement to Prevent Targeted Violence. U.S. Secret Service, Department of Homeland Security. Retrieved from: https://www.secretservice.gov/sites/default/files/reports/2024-10/Behavioral-Threat-Assessment-Units-A-Guide-for-State-and-Local-Law-Enforcement-to-Prevent-Targeted-Violence.pdf

BTAM teams operate before the violence can occur, ideally off-ramping behaviors before they require an emergency or crisis management response. In the event that violence does occur, the BTAM team should be engaged — after safety has been reestablished and the immediate crisis situation stabilized — to assess for any ongoing threat that the person of interest (POI) may pose and how to manage that threat. Even when a POI who engaged in an act of violence in a health care setting is arrested, adjudicated and incarcerated, that person likely will return to mainstream society someday. When that reintegration happens, the POI may seek health care services. The BTAM team should be available to inform the hospital or health system's plan for providing care safely and effectively.[101]

The BTAM Process

Receive a Report. The most robust workplace violence prevention and intervention programs build upon a leadership committed to creating a culture that promotes unhindered event reporting.[102] It is not incumbent upon persons who experience, witness or learn of concerning behavior to determine whether an event fits the definition of being an act of workplace violence or meets the criteria of being a threat. Such determination is the role of the trained multidisciplinary BTAM team. Rather, to overcome the highly problematic phenomenon of underreporting of violent behavior in health care settings, all persons in the health care environment (e.g., personnel, patients, visitors, etc.) should be encouraged to report any behavior that causes a safety concern.[103,104] Interestingly, health care personnel often do report violent events; however, they report them across numerous mechanisms that are not consistently consolidated and directed to a single multidisciplinary team.[105] It therefore matters that there should be "no wrong door" for event reporting and that a hospital or health care facility's reporting infrastructure consolidates all possible "front doors" into a single "BTAM room." Once event reports are received and the BTAM process commences, event reporters optimally will be notified that action is being taken and provided a point of contact for status updates.

Triage the Report. The first questions the BTAM team must answer upon receiving a report of behavior causing a safety concern are: "Does this situation pose an immediate life safety threat? Is anyone bleeding, dead or about to be?"

If the reported behavior represents an imminent or current crisis, then immediate intervention and appropriate emergency response protocols must be enacted. As previously noted, BTAM is not crisis management. If the reported behavior is not imminent but represents a possible future life safety concern, then the BTAM process progresses.

Assess the Threat. In its most basic form, threat assessment involves collecting dots and then connecting them to answer these questions: "Does the reported behavior pose a threat? If so, then a threat of what, by whom, toward whom and under what conditions?"

Obtaining accurate and thorough answers to those questions drives the next BTAM process elements.

Gather Initial Information. One of the many reasons BTAM is done by multidisciplinary teams is to increase the likelihood that all relevant information needed to answer the key assessment questions above is available to the BTAM team.[106] BTAM team members are uniquely positioned to be able to "collect the dots" that are relevant for completing a thorough assessment. Not all "dots" are available to all people, though. Health care professionals bring critical data to the BTAM process that is unavailable to other multidisciplinary team members, whereas hospital security personnel — interfacing ethically and legally with law enforcement personnel — bring equally critical but different "dots" to the BTAM team. When gathering essential information necessary for conducting a threat

---

101 Wyatt R, Anderson-Drevs K, Van Male LM. Workplace Violence in Health Care: A Critical Issue With a Promising Solution. *JAMA*. 2016;316(10):1037–1038. doi:10.1001/jama.2016.10384

102 The Joint Commission. (2021). R3 Report Issue 30: Workplace Violence Prevention Standards. Retrieved from: https://www.jointcommission.org/-/media/tjc/documents/standards/r3-reports/wpvp-r3-30_revised_06302021.pdf .

103 Ibid.

104 Hutton, S., Vance, K., Loftus, S., Roth, G., & Van Male, L.M. (2023). National Development and Implementation of a Democratized Disruptive Behavior Reporting System in Health Care. *Journal of Medical Systems*. https://doi.org/10.1007/s10916-023-01999-0

105 Ibid.

106 O'Toole, M.E. (2021). Fundamentals of Threat Assessment for Beginners. In International Handbook of Threat Assessment (2nd Ed.). Meloy, J.R., and Hoffman, J. (Eds). Oxford. (p. 355).

assessment, BTAM teams must be mindful of the difference between personnel- and patient-generated behaviors. Access to information varies based upon the role of the individual at the time of the behavior.[107]

Render Information. Using a Structured Professional Judgment (SPJ) approach is widely concurred to be the current best practice in BTAM. [108,109] One of the numerous benefits of using the SPJ approach is that a consistent, objective and empirically informed process for focusing the behavioral threat assessment on relevant factors can help guard against bias in the BTAM process. The BTAM process is only as good as the data informing it. As there may be bias in what is reported as the BTAM team must strive to be vigilant not to promulgate bias by having an objective assessment process.[110, 111, 112] The SPJ approach can be especially helpful in guarding against the lack of objectivity in threat assessment practices introduced by the phenomenon of emotional reasoning. In short, emotional reasoning is a human cognitive distortion wherein the degree to which a person believes a thought they have is true (regardless of whether it actually is factual) is directly related to the magnitude of that thought's co-occurring emotion. Emotions tend to run high when fear for life safety exists, and the strength of those emotions can sway the thinking of the BTAM team. By focusing the BTAM team's threat assessment process on empirically informed violence risk and protective factors, the SPJ approach helps overcome problematic emotional reasoning. When members of the multidisciplinary BTAM team become the targets of a POI's behaviors, then the affected BTAM members should recuse themselves from deliberations involving that POI. Even in cases wherein targeted BTAM members believe they are not falling prey to emotional reasoning, their continued engagement in the BTAM process will call into question the objectivity of the entire BTAM team's behavioral threat assessment and subsequent threat management interventions. When in doubt, step out.

There are numerous SPJ tools and instruments available in the public and proprietary domains. BTAM teams electing to use such a tool or instrument will be well served to ensure that the product chosen is standardized and/or normed for the health care patient or personnel population in which it will be used.[113,114] Additionally, the type of violence being assessed should align with the tool or instrument selected (e.g., the SPJ tool or instrument used to inform an understanding of the threat posed by a potentially radicalized individual to all personnel in a hospital is not the same tool or instrument that should be used to inform an understanding of the threat posed to a clinic by the intimate partner of an employee).

The BTAM team will be well advised to be mindful of the potential to "over-assess" the existence of the threat posed by a behavior. Figure 2 depicts the four possible outcomes of crossing a yes or no assessment of a life safety threat being posed with the yes or no reality of that violence occurring. A true positive and a true negative outcome are not problematic. The risk of over-assessing the threat posed by a POI's behavior emerges in the inverse relationship between a false negative and a false positive (see Figure 3). By definition, decreasing one type of error automatically increases the other type of error. In a BTAM team's quest to avoid the wholly undesirable outcome of assessing a POI's behavior as not posing a life safety threat, only to later have that POI engage in a devastating act of targeted violence, BTAM teams may fall prey to rendering an assessment that a life safety threat is posed when, in reality, it is not.

107 For example: Consider a case involving the alleged concerning behavior of a health care system employee who also receives health care at one of its hospitals. If the POI's behavior occurred while acting in an employee role, then accessing the health care record to gather information very likely constitutes a HIPAA violation; however, if the same behavior occurred while the POI was acting in the role of being a patient, then accessing the health care record is acceptable as such is done to inform the treatment plan for delivering safe and effective health care.

108 The Association of Threat Assessment Professionals (ATAP) defines structured professional judgment (SPJ) as a systematic methodology that combines evidence-based, empirically-validated risk factors with professional expertise to assess and manage threats of targeted violence.

109 Association of Threat Assessment Professionals (in press). RAGE-V (2nd Ed).

110 Sun M, Oliwa T, Peek ME, Tung EL. Negative Patient Descriptors: Documenting Racial Bias In The Electronic Health Record. Health Aff (Millwood). 2022 Feb;41(2):203-211. doi: 10.1377/hlthaff.2021.01423. Epub 2022 Jan 19. PMID: 35044842; PMCID: PMC8973827.

111 Ranapurwala, SI. Identifying and Addressing Confounding Bias in Violence Prevention Research. Curr Epidemiol Rep. 2019 Jun;6(2):200-207. doi: 10.1007/s40471-019-00195-4. Epub 2019 Apr 26. PMID: 32322458; PMCID: PMC7176054.

112 Sun, M., et al. Negative Patient Descriptors.

113 Heilbrun, Kirk, *Evaluation for Risk of Violence in Adults* (New York, 2009; online edn, Oxford Academic, 1 Jan. 2015), https://doi.org/10.1093/med:psych/9780195369816.001.0001, accessed 7 Dec. 2024.

114 Douglas, K.S., and Otto, R.K. (Eds). Handbook of Violence Risk Assessment (2nd Ed). New York, NY: Routledge, 2021.

Figure 2: Possible Outcome Combinations of Assessment vs. Reality of Life Safety Violence

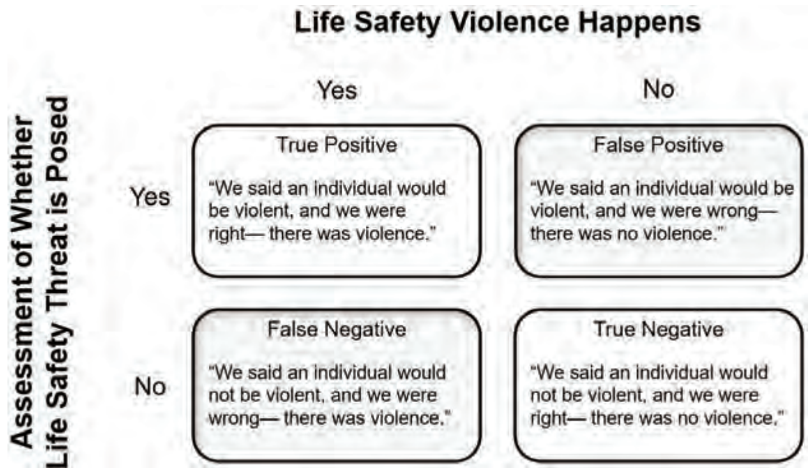
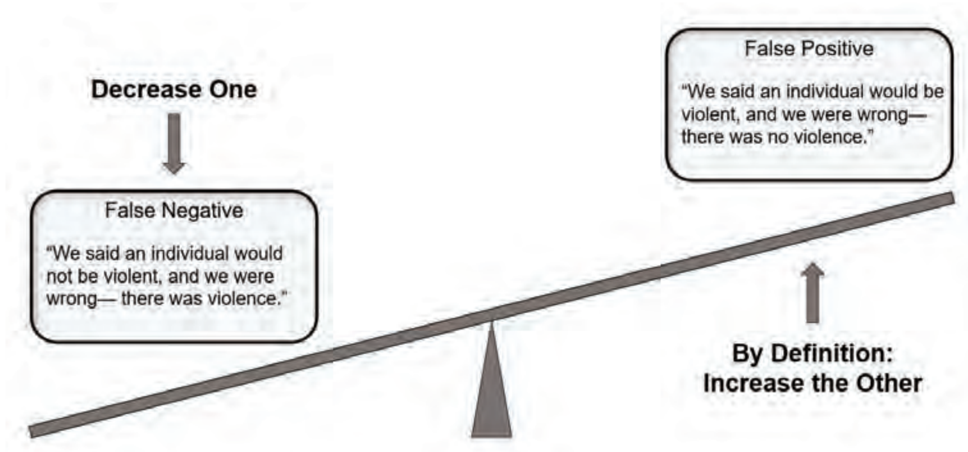


Figure 3. Inverse Relationship Between False Negative and False Positive



Manage the Threat. The BTAM process requires that a threat assessment must precede the development of a threat management plan. A common pitfall for newly formed BTAM teams is to move directly from receiving a concerning behavior report to attempting to manage it. Although it is understandable that BTAM teams want to take responsive action when individuals report behavior that may pose a life safety threat, bypassing triage and not completing a thorough assessment is dangerous. A properly conducted behavioral threat assessment allows trained BTAM teams to "right size" and align individualized threat management interventions with the threat posed by the behavior. By assessing *before* managing, BTAM teams uphold one of health care's primary tenants: First, do no harm.[115]

Develop and Recommend Interventions. Having addressed the key threat assessment questions above, the BTAM team now turns its focus to answering the following questions:

- Under what conditions does the POI pose the greatest threat?
- How can the BTAM team decrease the threat that the POI poses by increasing protective factors, reducing dynamic risk factors, or both?
- What are the POI's perceptions about the behavior that poses a safety threat?
- What level of engagement is possible for the POI to have in developing threat management interventions?
- How invested is the POI in adhering to recommended threat management interventions?

115 Van der meer, Bram. B, and Diekhuis, Margaret, L. (2014). Chapter 4 Collecting and Assessing Information for Threat Assessment in International Handbook of Threat Assessment, Meloy & Hoffman (Eds). Oxford (p. 58).

The uncomfortable reality in developing threat management interventions is that there is no one-size-fits-all, if-this-then-that guaranteed approach for ensuring life safety that works across all cases. Incorporating the following principles into developing behavioral threat management interventions may help BTAM teams operating in health care settings tolerate the ambiguity inherent in the Manage phase of the BTAM process.

Access to health care is a threat management intervention. Comprehensive threat management plans leverage increasing protective factors and reducing risk factors in the POI's life. Many of the protective factors that reduce the risk of severe violence occurring in a one-year period are brokered through health care access.[116,117] That said, it is legitimate for the BTAM team to consider threat management interventions that may change the following aspects of health care delivery:[118]

- When (e.g., time of day, hours of scheduled appointments, etc.)
- By whom (e.g., which health care providers are best suited to interact with the POI, how many providers, etc.)
- Where (e.g., in which physical location, clinic, department, building, hospital, etc.)
- How (e.g., via video or telehealth appointment, in an increased security presence in or more frequent rounding through the relevant care location, etc.)

Regardless of the necessity of any of these possible departures from traditional health care delivery practices, the goal of continuing the delivery of safe and effective health care for all persons in the setting remains primary.

People tend to support what they create. Whenever possible, involving POIs in creating safety strategies that they are willing to implement increases the likelihood that the threat management plan will succeed.

Beware rejection. Although it is an understandable human impulse to create distance (physical, psychological or emotional) from something or someone that causes fear, the practice of distancing used as a threat management strategy often is problematic. Depending upon the hospital or health care system's operating context, removing a POI from health care access may be illegal due to contractual (i.e., Medicaid care provision) or legislative requirements.[119] Removing a POI from health care access can have the unintended downstream consequence of the BTAM team losing the ability to maintain the data stream from the POI to monitor deviations from behavioral baselines. Further, excluding a POI from receiving health care does not necessarily decrease the life safety threat the POI may pose. Obtaining a personal protective or temporary restraining order — a form of rejection — is followed by an increase in violence 33% of the time.[120] Health care personnel considering using a restraining order as a threat management strategy may want to consider completing the "Restraining Order Worksheet" prior to seeking this intrusive intervention.[121] Rejection is a common trigger to violence, and losing access to health care represents a particularly intense form of rejection as it has the potential for real, or perceived by the POI, negative implications for future life quality, or even life quantity.

Align threat management interventions with the actual magnitude of the threat. Per the discussion in the Assess section above, there is potential for BTAM teams to inadvertently engage in over-assessing the threat a POI's behavior poses. When this error occurs, the commensurate next step tends to be that of over-managing the behavior. Rather than recommending the least restrictive or nonconfrontational threat management strategies, the BTAM

116 Elbogen, E. B., Cueva, M., Wagner, H. R., Sreenivasan, S., Brancu, M., Beckham, J. C., & Van Male, L. (2014). Screening for violence risk in military veterans: predictive validity of a brief clinical tool. *Am J Psychiatry*, 171(7), 749–757. https://doi.org/10.1176/appi.ajp.2014.13101316

117 Elbogen, E. B., Johnson, S. C., Wagner, H. R., Newton, V. M., Timko, C., Vasterling, J. J., & Beckham, J. C. (2012). Protective factors and risk modification of violence in Iraq and Afghanistan War veterans. *J Clin Psychiatry*, 73(6), e767–e773. https://doi.org/10.4088/JCP.11m07593

118 VA response to disruptive behavior of patients. 38 Code of Federal Regulations §17.107. Retrieved from https://www.govinfo.gov/content/pkg/CFR-2014-title38-vol1/pdf/CFR-2014-title38-vol1-sec17-107.pdf

119 Ibid.

120 Spitzberg, B.H. (2002). The Tactical Topography of Stalking Victimization and Management. Trauma, Violence, & Abuse, 3(4), 261-288. https://doi.org/10.1177/1524838002237330.

121 Ryan, S. (2015). Restraining Orders in Healthcare: Effective, Ineffective or Dangerous? Embracing Risk, Medical College of Wisconsin. Retrieved from https://www.mcw.edu/-/media/MCW/Departments/Risk-Management/Restraining-Orders-in-Healthcare.pdf

team that over-assesses the threat a behavior poses often opts for deploying interventions best suited for very acute, violence pathway-progressed, or imminent life safety threat cases.[122]

Account for context. The context in which behavior occurs can, does and will change. The same behavior in one context may represent a different level of posed threat than it would if it had occurred in a different context. For example, consider the behavior of bringing a handgun into a health care facility. The life safety threat this behavior represents must be considered in light of the context in which it occurs. Interventions appropriate for addressing one POI's behavior clearly would not be aligned with those required to manage the threat posed by another POI's behavior. The importance of context mandates that the BTAM team remains objective and develops individualized interventions that account for situational variables that differ across cases.

Consider the unintended downstream consequences of code of conduct letters and behavioral contracts. Many health care providers abide by the adage that if something was not documented, then it was not done. The desire to send code of conduct letters or behavioral contracts to POIs is understandable, as it gives the health care facility documentation that behavioral expectations — and consequences for not adhering to them — were clearly communicated. Such documents, however, may in and of themselves become fuel that feeds the fire of violence pathway progression. If a code of conduct letter or behavioral contract is determined to be necessary, then every attempt should be made to deliver it in a manner that allows for observing how the POI reacts and ensures opportunity for clarification and interpersonal connection.[123]

Decide on Interventions. Ideally, the trained members of the multidisciplinary BTAM team will have decisional authority to implement the threat management interventions they develop. In some health care settings, however, the BTAM team's recommended interventions may require formal approval by personnel not directly serving on the BTAM team prior to implementation. Knowing in advance the risk tolerance thresholds of approving personnel may help minimize processing delays. When developing threat management interventions, the BTAM team will want to consider the clinical, ethical, legal, financial, political, regulatory and optical implications of its recommended interventions. The BTAM team's strategy may be brilliant, but if elements of its plan fail along any of these dimensions and are subsequently not approved for implementation, then the entire threat management plan's effectiveness may be compromised. For example, retrofitting numerous structures on a multi-acre health care campus with ballistic glass may indeed be a potentially effective life safety strategy; however, the financial implications of this proposed intervention may render it a failed recommendation. Regardless of who approves threat management interventions, the BTAM team should document the recommendations it makes, clearly noting which interventions were approved for implementation.

Implement Interventions. All the BTAM team's work to this point in the process — all the time, expertise and resources invested in assessing the threat posed by a POI's behavior and developing individualized strategies for managing that behavior — risks becoming completely meaningless if no one knows what those strategies are. Personnel who will implement the BTAM team's recommended interventions must know what actions to take and under what conditions to best continue the delivery of safe and effective health care. The BTAM team therefore requires a reliable method for communicating life safety plan elements to all relevant stakeholders. In what has become a landmark study in health care violence prevention, Drummond et al. described an approach for reducing violent behavior incidents by 91.6% among a group of repetitively disruptive patients that involved placing an alert in the patients' electronic health record.[124] Policy guiding the ethical use of electronic health record alerts (EHRAs) should emphasize several points:[125,126]

122 Calhoun, F.S., and Weston, S.W. Threat Assessment and Management Strategies: Identifying the Howlers and Hunters (2nd Ed.). Routledge, New York: 2016.

123 Fiester A, Yuan C. Ethical Issues in Using Behavior Contracts to Manage the "Difficult" Patient and Family. *Am J Bioeth*. 2023 Jan;23(1):50-60. doi: 10.1080/15265161.2021.1974974. Epub 2021 Sep 30. PMID: 34590938.

124 Drummond DJ, Sparr LF, Gordon GH. Hospital violence reduction among high-risk patients. *JAMA*. 1989 May 5;261(17):2531-4. PMID: 2704113.

125 VHA Workplace Violence Prevention Program. U.S. Veterans Health Administration Directive 1160.08(1). Retrieved from https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=10280

126 Patient Record Flags. U.S. Veterans Health Administration Directive 1166. Retrieved from https://www.va.gov/VHAPublications/ViewPublication.asp?pub_ID=11547

- EHRAs must only be used to communicate information necessary to know during the initial moments of a health care encounter to promote safety. There must be a governed process for placing, modifying and inactivating EHRAs. Enacting an EHRA may only occur after conducting a thorough behavioral threat assessment and developing an individualized threat management plan. EHRAs must have an established review cycle to ensure they communicate relevant information over time. Once an updated behavioral threat assessment determines that an EHRA's usefulness for communicating a safety strategy has passed, then the EHRA should be deactivated. As a part of the medical record, EHRAs are releasable to other health care systems to promote care continuity and life safety across collaborative heath care networks.
- EHRAs themselves must be brief, objective, and only use non-inflammatory language. It is inappropriate for an EHRA to contain specific diagnoses or identify criminal status. For EHRAs to maintain their functional alert salience, they should not be over-used. Alert fatigue is a legitimate concern, thus EHRAs should be enacted judiciously.
- EHRAs must *never* be used as a means of punishing a patient for engaging in behavior that causes a safety concern. EHRAs are not a safety or threat management intervention in and of themselves. Rather, as noted above, EHRAs are a communication tool. EHRAs do not override sound clinical judgment for how or whether to provide health care. They must not be used as the sole reason for terminating a health care encounter. The existence of an EHRA must not be the singular criteria used for limiting a patient from accessing a clinically indicated procedure, program or service. Finally, as a tool intended to promote knowledge of how health care may be delivered safely and effectively, EHRAs should not be used for administrative, legal, or law enforcement purposes.

Monitor Impact. Once the threat management interventions are implemented, the BTAM team turns its attention to answering the following questions:

- Did it work?
- Did the threat management strategy have the desired effect on the POI's behavior?
- Has the threat posed by the POI been disrupted?

At this point in the BTAM process, the team returns to information gathering. This return to "collecting the dots" often necessitates a subsequent "reconnecting the dots" to incorporate new data and modify the threat management strategy accordingly. Thus, the BTAM process, by design, is ongoing and iterative. It ensures that the BTAM team is able to evolve and align its recommended life safety interventions based upon incorporating new data about the ever-changing threat landscape. The BTAM process continues for as long as the POI remains a safety concern to the BTAM team.[127,128]

Why Is BTAM Important for Hospitals and Health Care Systems?

Hospitals and health care systems no longer operate under the misconception that they are impervious to the threat of targeted violence.[129] The process for ethically determining the most effective approach to mitigate targeted violence threats in health care settings, however, may be difficult to confirm through traditional control group-based research. What hospital, health care system or clinic would accept being the location that receives absolutely no life safety threat mitigation resources in order to test the null hypothesis in such a study? Hospitals and health care systems therefore must rely upon the strength of practice-based evidence to support the life safety protection approaches it adopts. [130]

127 Van Male, L., Vance, K., Hutton, S., & Truman, B. (2018). Comprehensive Workplace Violence Prevention Program: Model and Process Success in a National Healthcare System. In I. Needham, K. McKenna, O. Frank, & N. Oud (Eds.), Proceedings of the Sixth International Conference on Violence in the Health Sector: Advancing the delivery of positive practice (pp. 464-470). Toronto: Oud Consultancy.

128 U.S. Veterans Health Administration. Disruptive Behavior Committee Guidebook. Retrieved from https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9690

129 Huffman, M.C., and Amman, M.A. (2023). Violence in a place of healing: Weapons-based attacks in health care facilities. *Journal of Threat Assessment and Management*, Vol 10(3), 151-187.

130 Ammerman, A., Woods Smith, Tosha, & Calancie, L. (2014). Practice-based evidence in public health: Improving reach, relevance, and results. *Annual Review of Public Health*. Vol. 35:47-63 (Volume publication date March 2014) https://doi.org/10.1146/annurev-publhealth-032013-182458

It is indisputable that targeted attacks occur in open access spaces (e.g., educational facilities, houses of worship, retail environments, entertainment venues, political settings, etc.).[131] Hospitals and health care systems address very similar security difficulties that other open access spaces face. Although hospital and health care facility designers strive to achieve open, welcoming and attractive physical environments created with the explicit goal of enhancing patient safety, the porousness of health care delivery spaces creates a challenge for ensuring their physical security.[132,133] Health care entities, having characteristics similar to those of other open access spaces, reasonably may inform their life safety strategies by applying what is already known to work in similar venues. By turning toward the BTAM process used to promote life safety by professionals working in other open access spaces, and by incorporating those venues' implementation hospitals and health care systems may avail themselves of learning obtained at the incalculable cost of lost human life.[134,135]

When implemented properly, the BTAM process is a robust and defendable approach for identifying, assessing and managing the threat of life safety violence posed by human behavior, and it works in hospital and health care settings.[136,137,138] As noted above, when a governed process was used to arrive at the decision to enact an EHRA as a strategy for communicating essential information at the initial moments of a patient's encounter to promote safety, violence recidivism was reduced in POIs known to pose a behavioral safety threat. The process that Drummond et al. used is the BTAM process: EHRAs may only exist if a proper threat assessment is conducted that informs a customized threat management strategy. Therefore, if EHRAs (a product of the BTAM process) are shown to be related to violence reduction in health care, then the BTAM process itself has evidence supporting its effectiveness in reducing violence in health care.

The question hospitals and health care systems now face is not whether we should use BTAM in health care. Rather, given our understanding of the effectiveness of the BTAM process and the robustness of the science supporting it, the question is whether hospitals and health care systems can afford not to use BTAM.

---

131 Follman, M. (2022). Trigger Points: Inside the Mission to Stop Mass Shootings in America. Dey Street.

132 Reiling J. Safe design of healthcare facilities. Qual Saf Health Care. 2006 Dec;15 Suppl 1(Suppl 1):i34-40. doi: 10.1136/qshc.2006.019422. PMID: 17142606; PMCID: PMC2464867.

133 DHS Safety and Security Resources for Health Care Providers, Including Pharmacies. (2024). Retrieved from https://www.dhs.gov/news/2024/02/26/dhs-safety-and-security-resources-health-care-providers-including-pharmacies

134 Ryan, S. (2023). What does the School Shooting Case of Cleveland v. Taft Union High School Mean for Threat Assessment Teams in Healthcare? Wisconsin Society for Healthcare Risk Management, Retrieved from https://www.mcw.edu/-/media/MCW/Departments/Risk-Management/Cleveland-v-Taft-Union-HS-Article.pdf

135 Ibid.

136 Amman, M., et al. Making prevention a reality

137 National Threat Assessment Center. Behavioral Threat Assessment Units

138 Drummond DJ, Sparr LF, Gordon GH. Hospital violence reduction among high-risk patients. JAMA. 1989 May 5;261(17):2531-4. PMID: 2704113.

Best Practices in Building and Supporting Threat Management Teams

John "Jack" Rozel, M.D.
Co-Director, UPMC Systemwide Threat Assessment and Response Team
Medical Director, resolve Crisis Services of UPMC Western Psychiatric Hospital
Professor of Psychiatry and Law, University of Pittsburgh

Behavioral threat assessment and management (BTAM) is an approach to preventing both targeted and stochastic violence that works effectively across a variety of contexts and scales both inside and outsidehealth care. Developing and supporting BTAM teams within health care centers has been identified as a critical tool to reduce violence in health care settings by the International Association of Healthcare Safety and Security and was recently identified by the National Council for Mental Wellbeing as the top a recommendation for hospitals to help prevent mass violence[139.140,141] Done properly, BTAM teams protect, support and serve the clinical, scientific and community service functions of modern health care systems.

Threat management integrates cutting-edge science with professional judgment and relies deeply on fostering collaboration inside and outside the team while maintaining a clear mission in the face of high-risk decisions in areas that can often extend beyond the structure of charted territory. The work of BTAM is deeply synergistic to the clinical, scientific and humanitarian mission of modern health care, but the work is not easy — and the work is all but impossible without effective executive support.

The best BTAM teams begin with four essential elements that strong executive leadership can champion: membership, mission, mandate and money. This section will provide strategic guidance for health care executives on how to sponsor and support high quality BTAM programs in their institutions.

Membership of Subject Matter Experts Who Excel on High Performance Teams

In many ways, building a BTAM team is like building a new clinical team: diverse professionals who are eager and effective team workers, and who are comfortable working with different disciplines in collaborative and adaptive process, brought together to meet a previously unaddressed need. More concretely, BTAM teams will need to be composed of experienced professionals from specific disciplines complemented with access to ancillary partners in other areas. Core disciplines seen in most threat management teams include behavioral health, security, law and human resources. Some of the most frequently tapped resources also include clinical operations and services, risk management, patient relations, compliance and complaints teams, employee assistance programs, and internal communications. Team members should be skilled in their core operational areas and adept at learning and integrating their work into the threat management model.

Core team members should be supported in spending a significant amount of their time on BTAM work — for direct case work, ad hoc meetings, and addressing strategic initiatives including program development, connecting with employees and partners inside and outside of the medical center, and continuous skill development. A rigid "fully scheduled day" with an identified specific window for threat management activities is incompatible with the variable and flexible nature of threat management work. Effective executives recognize the importance of threat management work and will ensure that team members have their time protected to do the direct case work and continue to develop professionally.

---

139 Medical Directors' Institute. 2024. "Mass Violence in America: Definition, Prevalence, Causes, Impacts and Solutions." Washington, D.C.: National Council for Mental Wellbeing. https://www.thenationalcouncil.org/resources/mass-violence-in-america-causes-impacts-and-solutions/.

140 Amman, M., & Meloy, R. (2022). Incitement to Violence and Stochastic Terrorism: Legal, Academic, and Practical Parameters for Researchers and Investigators. *Terrorism and Political Violence*, 36(2), 234-245. https://www.tandfonline.com/doi/full/10.1080/09546553.2022.2143352

141 "Threat Management." 2018. 1.09.03. IAHSS Industry Guideline. International Association for Healthcare Security & Safety.

BTAM is an integrated discipline which requires study, supervision and practical experience to do the operational work effectively. For example, this means that an attorney on the team needs to devote bandwidth both to continuing to develop and grow their skills as a health care attorney and developing as an effective threat management expert as well. For a behavioral health team member, this means maintaining a high degree of clinical competence in addition to developing their skills in BTAM. Put simply, BTAM team assignment should not be seen as a collateral duty or temporary assignment by the team members or their chains of command, but instead as a central role and commitment for their career and their organization.

It should also be noted that threat management work relies heavily on the professional judgment of its team members. The case work is fundamentally idiographic: Judgments are based on science and the experience of the team members but are applied to the individual being evaluated — often using incomplete information in an environment that is evolving quickly. In doing such work, the diverse perspectives, styles and approaches of the team are indispensable in producing more accurate assessments, more equitable processes and more effective interventions. This relies on a team that is diverse and mindful of the impact of personal and team dynamics on cognitive errors and biases in their decision making.

At a higher level, the membership question includes what business unit "owns" threat management. As noted, BTAM work is intrinsically multidisciplinary, with behavioral health, security, legal and HR all playing critical roles. BTAM's core values are close to clinical values, and fundamentally, stopping violence is about changing behavior; should BTAM fall under clinical services? BTAM's mission is intrinsically about protecting the mission and staff of the health center; does this mean that BTAM falls under security services? All employees have a right to reasonably safe workplaces, and most threat cases are about threats against employees; does this make BTAM an HR function? A good argument can be made for any of these decisions. Perhaps the deciding factor comes to the essential question of finding the right executive champion to own, sponsor and develop the threat management program for the organization. BTAM needs a champion who is both politically savvy and sincerely apolitical, focusing passionately on the mission and purpose that BTAM programs play within the organization.

A Mission That Is Clear, Protected and Responsive to the Needs of the Organization

Threat management is about protecting and supporting the clinical, scientific and community service mission of the health care organization from internal and external threats in ways which are evidence-based, ethical and applied fairly across the organization. For example, the widow of a patient who died at the hospital is blaming the treatment team for the death and is threatening to kill their families. Most will agree this is within scope for a hospital threat management team. In another case, the widow of a patient who died at the hospital where no errors were identified is demanding the hospital apologize and punish the doctor, and she has now approached the hospital CEO in the community demanding to discuss this issue further. Well, this may well be a threat management issue, or it may be better handled by the complaints and patient relations team.

BTAM teams generally prioritize protecting employees, patients and visitors from physical dangers from known or potential violent attacks. The margins can blur, and distinguishing between a reasonable extension of the subject matter expertise concentrated in the BTAM program to other service areas and mission creep can be challenging. Furthermore, when a staff member feels threatened, hospitals need to make it as easy as possible for them to quickly hand off their concerns to a party that can responsibly investigate and manage the issue, even if it is not a bona fide threat. The employee is under duress, may be in need of support or care themselves, and should not be expected to spontaneously navigate the complex pathways of health care systems on their own.

Just as calling a code should occur easily and with a relatively low threshold, so too should accessing the threat management team. At the same time, threat management teams cannot and do not replace existing business policies and systems for addressing workplace disputes, quotidian workplace violence and clinical agitation management, patient complaints, or social media discourse about a health system or its employees.

Much can be said in favor of a broader mission for threat management teams; however, broader missions require more resources, including financial ones, and possibly a different mandate. When initially developed, teams may do better with a narrow scope but will still need a mission and operational guidelines adhering to the principle of "when in doubt, be helpful." Over time, expanding the mission, scope and responsibility of a threat program may be the right business decision. Leadership champions for threat management programs need to help threat management teams effectively expand their mission when appropriate or help the organization develop other resources when needs are repeatedly identified beyond the scope of the threat management program. Again, politically savvy but apolitical team leadership can be indispensable in navigating the interactions with other parts of the health care system.

Mandate of Authority Within the Organization and the Community

Different organizations imbue their threat management programs with varying degrees of authority and power. Do they serve as consultants, providing added investigatory, decision-making and interventional tools to the leadership of a local business unit? This would be similar to a specialty team consulting on a patient admitted to another service at the hospital: They advise and support in the care of the patient, but decision-making authority and ultimate responsibility stays with the originating service. Generally, threat management teams are likely to be disinclined to assume leadership, managerial or operational responsibilities from other areas of the health system but having the ability to make appropriate and timely interventions in exigent situations is essential. Conflicts between local program management and the threat management team may occur and may not be resolved easily or quickly. For example, an outpatient clinic receives a call from an upset patient who threatened the doctor; the clinic wants the threat management team to call the patient and dismiss them from the practice, but the threat management team wants the clinic to call the patient to attempt to de-escalate and problem solve with the patient. A clear mandate about what the threat management team — and other business units' — responsibility is and is not, and clear operational guidance on resolving disagreements, should be explored. Part of this is simply good social and collegial skills, but having formal written regulations or policies to fall back on can be useful as well.

Threat management teams need to work quickly and have the authority to make decisions independently. An executive champion for a threat program should be well informed of the threat management team's activities at a level of detail that is practical but not onerous. The threat management team itself needs to be empowered and entrusted to make real-time decisions independently and know how and when to engage with other partners inside or outside of the organization without being delayed by other processes. This requires the threat management team to have a good practical knowledge of hospital policies, regulations and laws, as well as comfort in recognizing when exigent circumstances exceed what those tools can appropriately address. Meeting this mandate effectively requires team membership that blends good judgment, experience within the organizational culture and a track record of fostering good professional relationships inside and outside of the medical center.

Money Is Never the Mission — But There Is No Mission Without the Money

William Webster, former director of the FBI, once said, "Security is always seen as too much until the day it's not enough." Similarly, spending limited finances on security and threat management programs is easily seen as too much until it is recognized that it was not enough. Like so much of the organizational infrastructure that makes modern health care possible, threat management services are indirect expenses. A provider does not get to submit an enhanced billing code for an endoscopy because they needed to consult with a threat management team or have security on site for the procedure with a patient due to the patient's threatening history. Nonetheless, sometimes medically necessary services require just such expenses so that the patient can receive the needed care and staff can deliver that care in a reasonably and appropriately safe context.

Health care security is not free, but it is important to remember that a medical workplace that is reasonably safe requires paying for more than the physical facilities and engineering fixes like locks or doors. For threat management, this means more than just software and database systems for reporting and case tracking. It is more than just paying for ad hoc expenses for modifications to control access or adding a security presence for specific situations. It is also paying for the operational time of the threat management team to manage cases, communicate about their services to the system and support the continuous development of specialized threat management teams. It can also include the ability to retain and use other external resources including specialized consultants, investigators or close protection details as needed. For threat management programs to truly succeed in achieving the mission of providing a safe environment for the rest of the medical center staff to meet their clinical, scientific and community service missions, it also requires changes in organizational policies, practices and culture. Clearly, some of these elements are easier to capture in a budget than others.

Health care leaders are well versed in strategic budgeting and managing the seemingly endless indirect costs of health care services. The essential point is this: *Financially supporting security and threat management team expenses is vital to protecting the core mission of the medical center, and the costs of failing to apply resources proactively to these issues can have catastrophic consequences.* Even the best threat management team will ultimately fail if they do not have access to additional resources.

While deeper conversations can (and should) occur about offsetting indirect costs through general medical billing processes and public policy, using liability insurance premium discounts to offset and support threat management programs, and the role of the federal government in supporting public/private partnerships on security matters, the immediate issue every health care leadership team needs to immediately face is funding their threat management program.

Startup and ongoing operational costs will need to be addressed in different ways. Having intelligent, creative and engaged support from the financial team will be important at every stage of threat management team operations. And while it is likely a misuse of resources for threat management team members to spend excessive amounts of their time on budget and finance matters, it is also inappropriate for them to misuse the limited finances available to any health system. Put simply: Pay your threat management team to focus on their mission and provide them with savvy administrative support to handle the budget and financial needs.

Funding threat management programs in different systems will face different challenges. Threat management teams for a larger multistate medical system will look very different than a threat management team at a community medical practice. Both will need to devote resources and budget to threat management. The larger program will likely find that investing in their own robust internal threat management system makes the most sense; a smaller community hospital may be more reliant on consultants and ad hoc participation. *No health care system can afford not to invest in threat management teams.*

A Call to Action: Exercising Executive Power

Just as hospitals have remained focused on patient safety and quality over the past generation, so too must we now prioritize staff safety. Threat management teams play an essential role in staff safety and are a vital tool in protecting your medical center and its ability to fulfill the clinical, scientific and community service mission. Every health care leader should understand what their system does for threat management, how those programs are resourced, and who the executive champion is who is responsible for assuring that those teams have the membership, mission, mandate and money to succeed.

If your system already has a threat management program, then take time to learn more about what they do and have a sincere conversation with them about what resources they need to keep your organization safe. If your organization does not have a program, then find the executive champion in your organization who will foster the development of this team. This will involve finding the people with the right skills and disposition to do the work and supporting their journey to learn more about threat management to bring this essential practice to your center.

Effective Use of BTAM in Health Care Settings

Susannah Rowe, M.D.
Associate Chief Medical Officer for Wellness and Professional Vitality, Boston Medical Center
Chair, Wellness and Professional Vitality Advisory Council, Boston University Medical Group
Assistant Professor, Department of Ophthalmology, Chobanian & Avedisian School of Medicine

Robert A. Fein, Ph.D.
Forensic and National Security Psychologist
Consultant, FBI BAU-1

Concern about targeted violence in medical settings can take many forms. Several recent studies in medical literature suggest that physicians, nurses and other medical professionals and practitioners are often concerned about, and are responding to, risk of violent incidents in inpatient, outpatient and community settings. The underlying etiologies of these include intimate partner violence, stalking, grievance-based violence, gang-related violence and other interpersonal violence

Concerns related to violence — including decreased productivity, increased turnover and burnout — divert resources away from patient care at a time when health care settings are facing both increased demands for service and increased pressures for cost containment and reduction. How might hospitals and hospital systems respond to these pressing challenges?

We see two major benefits for development of thoughtful behavioral threat assessment and management (BTAM) programs in medical settings: 1) better understanding and prevention of potential violence, and 2) significant decreases in fear, stress and uncertainty for medical staff. Better understanding and prevention of potential violence develops when key players understand the range, patterns and types of violent incidents that may occur; the types of predicators or warning signs that may signal an event; and effective preventive and responsive measures to take. A decrease in fear, stress and uncertainty for medical staff can result when staff, managers and leaders know whom to consult about violence concerns and when they believe that the medical setting has the capacity to assess and mitigate potentially violent situations.

We propose that development of thoughtful and effective hospital-, city- and regional-based BTAM capacities may both reduce violent incidents and significantly decrease the worry level of medical and hospital employees, thereby likely improving morale.

Below are some fictitious vignettes that help to illustrate the range of threatening experiences and potential responses by health care staff in medical settings:

1. A clinic employee is terminated for poor performance and leaves a frightening note on their supervisor's desk stating, "You will regret this!" The supervisor shares the note with their human resources representative and the employee union.
2. A nurse goes to their supervisor stating that one of the nursing students has recently left their spouse and is staying with a sister. The nurse says that the student's spouse is very angry and has made threatening comments. The spouse knows where the student works and is known to own a gun. The nursing student spoke with their student advisor, but the advisor wasn't sure what to do. The supervisor calls public safety.
3. A new doctor takes over a practice and inherits many patients who are on narcotic pain medications. The doctor determines that one of the patients has been getting narcotics from several different practices simultaneously. At the next visit, the doctor declines to write a new controlled substances prescription. The patient storms off, yelling at everyone in the practice and saying that they will "pay for this." The office manager tells the security guard at the entrance to the building.
4. A patient undergoes cosmetic plastic surgery and is unhappy with the results. The surgeon refers the patient for second and third opinions, both of whom say the surgical result appears to be excellent. The patient declines to seek care with a different doctor and begins messaging the surgeon through the patient portal

almost daily with increasingly angry and threatening messages. The surgeon starts worrying about their safety when walking to and from their car. The surgeon contacts the patient safety and quality department and the patient experience team to ask how they should handle the situation.

5. A teenager is gravely injured after an altercation at a party. It has become clear that the patient is likely to die. An environmental services worker overhears a family member saying, "If they die, I'm going to make the other kid pay for what they did." The environmental services worker tells their supervisor.
6. A medical assistant (MA) becomes uncomfortable with a patient because they keep bringing in small gifts and asking the MA inappropriate questions about their personal life. Recently, the patient found the MA on Facebook and sent a friend request. At the last visit, the patient mentioned that they knew where the MA lives and suggested that the MA might run into the patient in their neighborhood sometime soon. The MA is directed to the legal department to find out how they should handle the gifts; MA mentions to the legal team the Facebook invite and cites concerns regarding the comments about running into each other outside of work.
7. A surgical tech is worried about a co-worker who is becoming increasingly erratic at work. The co-worker has been complaining about their boss in threatening language. The co-worker is former military, and a cafeteria worker has seen a hunting knife in their locker. The surgical tech mentions their worry to a friend at work.
8. A patient who has been seeing a licensed mental health worker for several years begins experiencing a psychotic break with delusions that their clinician is reporting them to the FBI. The patient becomes increasingly paranoid, believing that their medication is poisoned, so they stop taking it. The patient has come into the office several times demanding to see the social worker. They have also made several statements in front of the registration staff that their spouse is not safe at home with them. The mental health worker seeks advice from their department chair.
9. A family medicine resident has just moved across the country for training. They had a stalker from their hospital in a prior state, and they have a restraining order in that state. They are not sure what can be done to help keep them safe in their new location. They go to the local police station in their town to ask.
10. A gang-related incident has left multiple people hospitalized. A patient's visitors have tattoos that also are known to be gang-related. A cafeteria worker overhears members of this group making comments about how they will get revenge if their friend doesn't do well. The cafeteria worker tells their spouse about it that night.

These examples illustrate the range of potential threats that a hospital or health system may encounter on a regular basis. What threat assessment and management approaches might help with the above situations? We suggest consideration of a multi-tier BTAM program or "system" that 1) functions within a given hospital or medical setting and 2) links a number of hospitals/medical settings within a given city or region. Such a system would include a designated threat assessment and management team in each given hospital, supported by a city or region-wide threat assessment and management team for particularly concerning, complicated or multi-center cases.

As other sections in this guide suggest, a hospital-based BTAM would include a range of professional expertise, including hospital security personnel. Other members may include behavioral health and patient safety experts, as well as representatives from the patient experience team, front line staff and managers. Together, team members can prepare to evaluate and provide an immediate response to potential threats. Hospital practitioners and employees would have clearly understood ways to contact, seek consultation from and bring situations of concern to the in-house team. The team would have relationships with local governmental units, like the police department or social service programs, that it could call upon when appropriate. A hospital-based BTAM team could educate local "bystanders" about how to respond to concerns about violence.

A hospital-based BTAM program could provide guidance — and, if needed, intervention — in the cases described above. For situations deemed to be higher risk, more sophisticated consultation and intervention might be needed. A comprehensive BTAM system in a city or region might have a "high-level" pooled team composed of representatives from a number of hospitals that could provide expert consultation in cases that seem particularly complicated. Such a team would have representatives on it from city or county law enforcement agencies. It would develop and maintain relationships with other city or county threat assessment and management teams. This team might also have a liaison relationship with state and federal law enforcement organizations that respond to risk-of-violence situations.

A city-wide or regional hospital team would be sensitive to the particular kinds of threat situations that arise in medical settings. It would be able to draw on the expertise of other professionals who more regularly deal with threat-of-violence cases and could recommend special expertise to local hospital teams when needed.

A pooled team could serve as a "center of excellence" for hospital and medical-setting knowledge about BTAM. It would foster sharing of specialized expertise across the community. Such a team could serve as a repository for the range of risk-of-violence concerns present in an overall hospital community. As problems are solved, a city-wide or regional team could offer innovative ideas gleaned from both local and national sources to the hospitals in its area. A pooled team could distribute information from national resources, such as the FBI's Prevent Mass Violence campaign.

Targeted violence is, and likely will continue to be, a significant problem in our nation, including in hospital and medical settings. Thoughtful development of BTAM teams that focus on medical settings and practitioners is one step in responding to the risk of targeted violence attacks and the concerns that such violence brings.

Building Behavioral Threat Assessment and Management Teams Within Hospital Settings

Jennifer Tillman
Crime Analyst, FBI BAU-1

Behavioral threat assessment and management (BTAM) is continuing to be adopted in many arenas across our country, including schools, businesses, communities, government agencies, nonprofits and faith-based organizations. Hospitals are no exception. The importance and value of implementing a robust BTAM team is becoming increasingly recognized in every facet of society. After mass shootings and other violent attacks, it's common for warning signs to be uncovered that identified an individual was progressing towards an act of targeted violence. A unique factor about BTAM is that it seeks to identify whether someone may be progressing towards targeted violence *before* an incident occurs. The following are four key concepts or the four E's — educate, employ, establish and execute — that are fundamental to implementing a successful BTAM program within the hospital setting.

Educate Hospital Executives Regarding BTAM

First and foremost, BTAM needs support from executive management within any setting. It's vital that executives at every level understand and appreciate the utility of BTAM in health care. The evolution of the threat has led to increasing public expectation and responsibility on organizations and agencies to intervene in a way that prevents a mass attack before it occurs. We have tools to operate in the preventative space; because of those tools we have a growing obligation to use them to save lives. While developing local BTAM capability involves an upfront time investment, having access to BTAM resources allows hospital staff to streamline their response to critical incidents, rather than reinventing the wheel every time a concerning case comes in.

Employ Multidisciplinary Representation

BTAM necessitates *multidisciplinary* involvement of various functional stakeholders within an organization. Having multidisciplinary involvement might be one of the most critical factors for a BTAM program. Whether the hospital has a more global BTAM team, a specific patient threat assessment and management team (PTAMT) or multiple teams, all should include members whose functions holistically represent the overall organization of the hospital. Multidisciplinary involvement can leverage the capabilities, perspective and expertise of various disciplines to aid in effectively assessing concerning behaviors and to develop threat management strategies. The more well-rounded a threat management team, the more insight into the concerning behaviors and the better the outcome. Start small — but start.

Establish Necessary Team Structure and Organization

Highly effective teams facilitate collaboration, coordination and communication across various parts of organizations or communities to address persons of concern and threats of targeted violence. In most settings, this efficiency is accomplished with two teams: the core team and the affiliate team.

The core team will vary depending on the size of the hospital. In general, the core team will be comprised of key operational stakeholders — the senior clinician, legal counsel, risk management and security or law enforcement connected to the hospital. Other members can include patient safety, facilities, health and safety, the union and other relevant partners.

The affiliate team is a broader group of stakeholders who can be educated on BTAM concepts, refer cases to the core team when needed and be leveraged to support the core team on an ad hoc basis. The affiliate team could include law enforcement partners who don't have the resources to sit on a core team but may also contain private sector partners and other non-law-enforcement community stakeholders.

Execute BTAM Best Practices

In health care, the BTAM teams have numerous roles, but the primary one is to identify concerning behaviors and mitigate the threat. When an assessment is made regarding a case, the issue is far from concluded. Cases are rarely, if ever, completely resolved. They require regimented management and monitoring over time. An assessment is only as useful as the information in hand at any given time. As new information becomes available, assessments can and should be updated, and management and intervention should be adjusted accordingly. The key, however, is that cases are routinely reviewed over the course of weeks, months or even years.

Conclusion

BTAM is considerably useful and central to a comprehensive PTAMT within the hospital setting. With executive support, a multidisciplinary team utilizing a core and affiliate structure and implementation of best practices will ensure success across any hospital setting.

Legal Considerations for HIPAA and BTAM Teams in Hospitals: Working With Law Enforcement While Following HIPAA

Angel Gray
Director of Threat Assessment and Threat Management
University of North Carolina at Chapel Hill

In the complex relationship between public safety and patient privacy, hospitals and law enforcement must carefully navigate cooperation and compliance within the context of the Health Insurance Portability and Accountability Act (HIPAA). HIPAA was enacted in 1996 to enhance the efficiency and effectiveness of the health care system. It mandated the Department of Health and Human Services (HHS) establish national standards for electronic health care transactions and security of patient information. In December 2000, HHS introduced a set of regulations to govern the privacy of patient information known as the Privacy Rule, which was later revised in August 2002. The Privacy Rule sets minimum standards for protecting personal health information and applies to "covered entities," which include health plans, health care clearinghouses and health care providers such as hospitals. The aim of the rule is to safeguard individuals' health data while facilitating the flow of necessary health information to coordinate care and provide for the protection of the public. Hospitals must keep in mind that the Privacy Rule establishes the baseline for safeguarding patient data and supersedes any state laws that contradict its privacy provisions. However, other federal or state laws offering more extensive confidentiality protections for patient data, which do not conflict with the Privacy Rule, are not preempted and must be followed by covered entities.[142]

The information in this section is provided as a general guide for both hospitals and law enforcement officials. It is not intended to provide a comprehensive review of the HIPAA Privacy Rule, nor does it aim to explore every potential interaction between health care providers and law enforcement. Hospitals are encouraged to consult with their own legal counsel and compliance teams before finalizing any policy on the release of protected health information.

Despite its intent, the HIPAA Privacy Rule is commonly perceived and often cited as an obstacle to sharing information. In reality, the Privacy Rule strikes a sound balance of supporting individual control over information while removing barriers to coordinated care and enhancing flexibility for disclosures in emergency situations or threatening circumstances.[143]

As part of compliance efforts, hospitals can prioritize the necessary measures to safeguard patient information while concurrently maintaining a strong focus on the protection of their own staff and the public from acts of violence. The HIPAA Privacy Rule encourages cooperation between hospitals and law enforcement through multiple avenues for collaboration in the context of information sharing.[144] This cooperation aims to safeguard both staff and the public, and it is essential for both parties to work in unison to meet these responsibilities.

In recent years, there has been a significant increase in the use of behavioral threat assessment and management (BTAM) teams by law enforcement agencies.[145,146] These multidisciplinary teams, often comprising psychologists, law enforcement officers and legal professionals, play a crucial role in identifying, assessing and managing potential threats to public safety. BTAM provides a structured approach to evaluate the severity of a threat, the likelihood

142 U.S. Department of Health and Human Services (HHS); Office of Civil Rights [OCR]. (2003) Summary of the HIPAA Privacy Rule. Washington, DC: [Online]. Accessed: Summary of the HIPAA Privacy Rule | HHS.gov.

143 Ibid.

144 Ibid.

145 Ennis, L., Hargreaves, T., & Gulayets, M. (2015). The integrated threat and risk assessment centre: A Program evaluation investigating the implementation of threat management recommendations. *Journal of Threat Assessment and Management*, 2(2), 114–126. https://doi.org/10.1037/tam0000040.

146 James, D. V., & Farnham, F. R. (2016). Outcome and efficacy of interventions by a public figure threat assessment and management unit: A mirrored study of concerning behaviors and police contacts before and after intervention. *Behavioral Sciences & the Law,* 34(5), 660–680. https://doi.org/10.1002/bsl.2255

of its occurrence and the resources required to mitigate it.[147,148,149] The BTAM team's work is pivotal in preventing incidents of violence, ensuring public safety and maintaining social order. As such, the expansion of BTAM reflects law enforcement agencies' commitment to proactive and preventive measures in public safety management and is another avenue for collaboration between health care providers and law enforcement. For effective collaboration, hospitals and law enforcement agencies need to have a good understanding of the Privacy Rule, its purpose and its practical application to real world situations when information needs to be shared.

Receiving Information from Collateral Sources

First and foremost, hospitals and other care providers should note that the HIPAA Privacy Rule and other regulations governing protected health information do not limit the information providers can receive from collateral sources. Even without an apparent exception for information disclosure or patient authorization, providers can still receive information from collateral sources such as family members, other providers and law enforcement. This information is often vital for informing treatment decisions, deciding on appropriate discharge disposition and determining if disclosure of information is permitted. It can also assist in assessing dangerousness under involuntary commitment law and determining if the patient poses an imminent danger, indicating that the threshold for information sharing has been met or a duty to warn has been triggered. Ultimately, more information enables providers to make better decisions about patient care, treatment and disposition, ensuring everyone's safety — including the patient's.

As a general rule, HIPAA requires hospitals and other covered entities to safeguard patient information as confidential and only disclose that information in accordance with the regulations (45 CFR §164.502, 2003).[150]

To ascertain whether a disclosure of patient information to law enforcement is permissible, hospitals can follow a simple three-step analysis:

- **Has the patient authorized release of the information in question?**
  When trust is established, individuals are more likely to share their health information with agencies they believe offer essential or beneficial resources.[151,152] Law enforcement agencies, particularly those with dedicated threat assessment teams, are increasingly acknowledging the benefits of building rapport and trust with a potentially concerning patient or intended victim in the context of threat mitigation investigations. If law enforcement needs to communicate with a patient or access their information, the patient may agree to the hospital revealing their health information, assuming the law enforcement agency has devoted time to fostering this trust. Hospitals can then safely disclose the patient's protected health information specified in a written authorization for releasing such information. (45 CFR § 164.508, 2003).[153]
- **In the absence of patient authorization, is the disclosure required by law?**
  Even without a patient's express authorization, there are numerous instances in which hospitals are mandated to release protected health information to law enforcement or other public safety agencies. For example, the HIPAA Privacy Rule permits hospitals and other covered entities to comply with other federal and state laws that require disclosure of potential child abuse and neglect (45 CFR § 164.512(b)(1)(ii), 2003) and injuries such gunshot wounds (45 CFR § 164.512(f)(1)(i), 2003). Covered entities are also allowed to comply with court orders or other legal process such as when an investigator serves a court order or warrant to obtain patient information during a criminal or threat

147 Amman, M., Bowlin, M., Buckles, L., Burton, K. C., Brunell, K. F., Gibson, K. A., Griffin, S. H., Kennedy, K., & Robins, C. J. (2017). Making prevention a reality: Identifying, assessing, and managing the threat of targeted attacks. U.S. Department of Justice, Federal Bureau of Investigation.

148 Fein, R. A., & Vossekuil, F. (2000). Protective intelligence and threat assessment investigations: A guide for state and local law enforcement officials. National Institute of Justice.

149 Meloy, J. R., & Hoffman, J. (Eds.). (2016). International handbook of threat assessment. Oxford University Press.

150 U.S. Department of Health and Human Services (HHS); Office of Civil Rights [OCR]. (2003) Summary of the HIPAA Privacy Rule. Washington, DC: [Online]. Accessed: Summary of the HIPAA Privacy Rule | HHS.gov.

151 Platt, Jodyn E., Jacobson, Peter D., and Kardia, Sharon L.R. (2018) HSR: Health Services Research 53:2 Health Research and Educational Trust DOI: 10.1111/1475-6773.12654 RESEARCH ARTICLE.

152 Rasiah, S., Jaafar, S., Yusof, S., Ponnudurai, G., Chung, K. P. Y., & Amirthalingam, S. D. (2020). A study of the nature and level of trust between patients and healthcare providers, its dimensions and determinants: A scoping review protocol. *BMJ Open*, 10(1), e028061. https://doi.org/10.1136/bmjopen-2018-028061

153 U.S. Department of Health and Human Services. Summary of the HIPAA Privacy Rule.

assessment investigation (45 CFR § 164.512(f)(1)(ii), 2003). Even if a crime has not yet occurred, a duly authorized judicial official determining that the relevant legal criteria have been met may issue a court order mandating disclosure. Additionally, legal processes that require the release of patient information can occur through various administrative procedures provided the information sought is relevant and material to a legitimate law enforcement inquiry (45 CFR § 164.512(a)(1), 2003). Disclosures based on statute or legal process are typically mandatory.

In jurisdictions that recognize an affirmative duty to warn, health care providers are permitted, and sometimes required, to alert third parties if they believe in good faith that their patient presents a serious and imminent threat to their own safety or that of others (*Tarasoff v. Reg. Univ. of Calif.*, 1976; 45 CFR § 164.512(j)(1)(i), 2003).[154] This duty is rooted in common law and its application varies by state, with some states mandating such a warning and others merely allowing it. Importantly, the HIPAA Privacy Rule does not prohibit health care providers from fulfilling this duty to warn when applicable as discussed in further detail below.

- **In the absence of patient authorization and a legal requirement to disclose, is the disclosure otherwise permitted by the regulations?**
  When there is no legal requirement to disclose information, hospitals can still share protected health information with law enforcement in specific investigative or emergency situations. These disclosures generally fall into two main categories: information related to public health, national security and criminal investigations; and threats to safety.

Public Health, National Security and Criminal Investigations

The following disclosures are permitted under the Privacy Rule and are allowed as long as they are not prohibited by other state or federal law or professional ethical obligations:[155]

1. In response to a bioterrorism threat or public health emergency (45 CFR § 164.512(b), 2003).
2. To federal officials authorized to conduct intelligence and other national security activities (45 CFR § 164.512(k)(2), 2003) or to provide protective services to the president and others and conduct related investigations (45 CFR § 164.512(k)(3), 2003).
3. To report information that the covered entity in good faith believes to be evidence of a crime that occurred on the premises (45 CFR §164.512(f)(5), 2003).
4. To alert law enforcement to the death of a patient when there is a suspicion that death resulted from criminal conduct (45 CFR §164.512(f)(4), 2003).
5. To report information about a patient who is a crime victim if either the patient authorizes the release or if the patient is unable to grant authorization and immediate release is necessary to avoid adversely affecting law enforcement activity (45 CFR §164.512(f)(3), 2003).
6. If necessary, to alert law enforcement to criminal activity when responding to an off-site medical emergency (45 CFR § 164.512(f)(6), 2003).
7. Limited identifying information for purposes of identifying or locating a suspect, fugitive, material witness, or missing person (45 CFR §§164.512(f)(2), 2003).

As of June 25, 2024, a modification to the Privacy Rule requires law enforcement agencies to provide an attestation under certain circumstances. This applies when they request access to protected health information potentially linked to reproductive health care. The attestation is needed if the information is intended for use in administrative or judicial proceedings or specific law enforcement scenarios, such as crimes occurring on hospital grounds (45 CFR §164.512(f), 2003). The attestation must confirm that the information will not be used for any of three prohibited purposes:

1. To conduct a criminal, civil or administrative investigation for the act of seeking, obtaining, providing or facilitating reproductive health care

154 *Tarasoff v. Regents of University of California*, 17 Cal. 3d 425 (Cal. 1976).

155 U.S. Department of Health and Human Services (HHS) (2003) Standards for privacy of individually identifiable health information; Final rule. 45 CFR Parts 160 and 164. *Federal Register*, 68(34), 8334-8381. Accessed: https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C

2. To impose civil, criminal or administrative liability on someone simply for seeking, obtaining, providing or facilitating reproductive health care
3. To identify any person for any purpose described in the two instances noted immediately above. (45 CFR 164.502(a)(5)(iii), 2003)

Law enforcement officers are only required to provide an attestation in the absence of patient authorization for information disclosure. A provider's good faith reliance on such an attestation is permissible to provide the requested information (45 CFR §164.509, 2003).

Threats to Safety

In addition to the listed specific disclosures noted above and perhaps most relevant to working with law enforcement threat assessment teams, a covered entity may disclose protected health information, including psychotherapy notes, if it believes in good faith that the disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of the patient or others (45 CFR § 164.512(j)(1)(i), 2003).[156] The disclosure should be made to a person or persons reasonably capable of preventing or lessening the threat.[157] For instance, if a patient makes a credible threat to cause serious and imminent bodily harm to one or more individuals, the health provider can notify law enforcement, family members, school administrators, campus police or anyone else who might be able to prevent or mitigate the risk.[158] The Privacy Rule explicitly allows covered entities to rely on a credible report from an individual who seems to have knowledge of the potential threat posed by the patient (45 CFR § 164.512(j)(4), 2003).[159] As previously emphasized, it is vital to consider all information available from auxiliary sources, such as law enforcement agencies, when determining if an individual presents a threat.

For disclosures of protected health information, such as those highlighted above, not made pursuant to patient authorization or required by law, covered entities may only disclose the minimum amount of information necessary to fulfill the purpose of the request (45 CFR §§164.502(b), 164.514(d), 2003). The Privacy Rule's minimum necessary requirement is not a rigid standard and allows room for professional judgment and collaboration in making this decision.[160] While covered entities must independently evaluate the extent of protected health information that is reasonably required for a specific purpose, they may reasonably rely on representations made by a law enforcement official with respect to the amount of information he or she feels is necessary to fulfill the purpose of the request (45 CFR §164.514(d)(3)(iii)(A), and § 164.514(h), 2003). Hence, the Privacy Rule encourages a balanced approach to the "minimum necessary" requirement.[161] It promotes adherence to recognized best practices to prevent unnecessary information disclosure. At the same time, it supports collaboration with law enforcement agencies to identify the information needed to safeguard patients, staff and the public.

Other Laws and Ethics Codes

Based on the analysis above, hospitals should have the ability to navigate the sharing of information with law enforcement under the HIPAA Privacy Rule. There are a few additional considerations hospitals should bear in mind prior to sharing information. As previously stated, the HIPAA Privacy Rule provides for the minimum standards to protect patient health information and covered entities must also consider any existing federal or state laws or regulations that offer greater patient privacy protection before disclosing any information.[162] An example of such a regulation is the Confidentiality of Substance Use Disorder Patient Records regulations found at 42 CFR Part 2.[163]

---

156 U.S. Department of Health and Human Services (HHS); Office of Civil Rights [OCR]. (2003) Summary of the HIPAA Privacy Rule. Washington, DC: [Online]. Accessed: Summary of the HIPAA Privacy Rule | HHS.gov.

157 Ibid.

158 Ibid.

159 Ibid.

160 Ibid.

161 Ibid.

162 U.S. Department of Health and Human Services. Summary of the HIPAA Privacy Rule.

163 Confidentiality of Substance Use Disorder Patient Records, 42 CFR Part 2, Jan. 18, 2017, Accessed: https://ecfr.io/Title-42/Part-2.

These regulations stipulate that information related to substance use disorderdiagnosis and treatment can only be disclosed to law enforcement with the written authorization of the patient (42 CFR § 2.12(a), 2017). Exceptions include situations where a crime has been committed on the premises of the treatment facility, instances of child abuse or when there is an appropriate court order (42 CFR § 2.12(c)(5), § 2.12(c)(6), and § 2.61, 2017).

Another example would be professional ethical codes and state laws or regulations that provide for greater confidentiality protections for mental health treatment information. These ethics provisions and state laws vary by profession and jurisdiction and may limit the permissible disclosures to law enforcement to a greater extent than the HIPAA Privacy Rule. Fortunately, most states' statutes and ethical codes permit permissive disclosure of patient information in situations of emergency or imminent danger, even if there is no affirmative duty to warn. Prior to releasing information to law enforcement, hospitals should be mindful of these additional restrictions and consult with legal counsel.

Personnel Information

While beyond the scope of this guide, it is important to remember that HIPAA does not govern access to or release of employee personnel records. Therefore, hospitals must be acutely aware of the applicable laws governing release of their employees' confidential personnel information in situations where their staff may be a person of concern or an intended target of violence. Typically, employee personnel information is deemed confidential under state or local laws and can generally only be disclosed with the explicit consent of the employee. However, there may be certain scenarios where confidential personnel information may be shared with law enforcement, even without the employee's consent. Because these scenarios may vary by jurisdiction, it is crucial for hospitals and their lawyers to be aware of the personnel laws applicable in their locations. This knowledge will enable them to ascertain if and how they can share confidential employment information to ensure the protection of the public.

In conclusion, the cooperation fostered by the HIPAA Privacy Rule between hospitals and law enforcement in sharing information is paramount to ensuring public safety. This collaboration bridges the gap between health care and security, enabling a comprehensive approach to safeguarding our communities. It allows for swift action in emergencies, efficient handling of potential threats, and development and implementation of effective prevention strategies.

Law Enforcement BTAM Teams: What Hospitals Should Know

Karie A. Gibson, Psy.D.
Supervisory Special Agent, Unit Chief, FBI BAU-1

The first contact between law enforcement and medical setting personnel is often after a crime, such as a physical assault or a threat, has occurred. Traditionally, due to patient care privacy laws and confidentiality, medical settings are siloed from law enforcement. Due to these silos, many medical personnel may not be knowledgeable about the proactive measures law enforcement organizations are taking to address the threat of mass casualty targeted violence. Around the country, law enforcement agencies are establishing behavioral threat assessment and management (BTAM) teams to expand law enforcement options when they encounter a person of concern who may be contemplating targeted violence. Having BTAM teams established by law enforcement allows for multiple lines of interventions. Many times, these interventions for mitigation could be implemented before traditional criminal justice options become available or included with court mandated requirements. These BTAM teams allow options for mitigation before a crime has occurred, taking away the old adage, "No crime has been committed" or "Nobody has been hurt yet." As members of the community, we can do better — and we should.

A National Resource Available to Local Law Enforcement

The FBI's Behavioral Analysis Unit-1 (BAU-1) has a long history of operationally supporting our local, state and federal law enforcement partners to prevent terrorism and targeted violence. In 2010, BAU-1 created the Behavioral Threat Assessment Center (BTAC), which leads the FBI's efforts to organize, coordinate and synchronize an enterprise-wide strategy to incorporate BTAM principles into the FBI's objective of preventing acts of terrorism and mass casualty targeted violence. When implemented properly, BTAM principles are designed to prevent acts of terrorism and targeted violence before they occur, consistent with the FBI's authority to disrupt, mitigate and prevent federal crimes and threats to the nation's security. Integral to BTAM concepts is the need to develop and leverage partnerships and relationships across all levels of government and with nontraditional law enforcement partners, such as mental health, probation and parole, and social services.

Specifically, the BTAC is a national-level, multi-agency, multidisciplinary task force focused on the prevention of terrorism and targeted violence through the application of behaviorally based operational support, training and research to assist our local, state and federal law enforcement partners with prevention efforts. In this unique capacity, the BTAC provides investigative and operational support for the FBI's most complex, concerning and complicated international and domestic terrorism investigations. In addition, the BTAC provides threat assessment and threat management support to federal, state, local, tribal and campus law enforcement partners, as well as community stakeholders, working diligently across the United States on targeted violence prevention. Significant lines of effort on targeted violence prevention include persons of concern, potential active shooters, school shootings/threats, stalking and workplace violence. The BTAC's extensive and broad-ranging capabilities are enhanced through a cadre of BAU coordinators and threat management coordinators assigned to all 56 field offices across the United States. The BTAC is staffed by agents, analysts, mental health professionals and researchers from the FBI, the Bureau of Alcohol, Tobacco, Firearms and Explosives, U.S. Capitol Police and the Department of Defense.

The BTAC engages in operational support to the most concerning law enforcement cases around the country, assessing over 380 persons of concern annually and developing strategies to manage the threats they pose. In cases where a mass casualty event has occurred, the BTAC deploys to assist local investigators in determining what may have motivated a particular offender. Additionally, BTAC has published landmark academic research on pre-attack behaviors of active shooters and lone offender terrorists.

At each of the 56 FBI field offices, threat management coordinators are working to establish BTAM resources and teams in their communities. Local resources focus on the prevention of mass casualty targeted violence every day as law enforcement BTAM teams are working to build bridges with their community stakeholders. Many times, the BTAM teams will meet quarterly with their community stakeholders to share information, provide training and build partnerships with the shared goal of preventing mass violence. Medical settings are a stakeholder in the community that should be included in these partnerships with law enforcement. Further, medical personnel in key positions should seek out partnerships with their local law enforcement partners. During a mass casualty incident is not the time to meet your law enforcement leadership. Taking steps to proactively build a partnership between medical settings and the law enforcement who serve your area is the preferred practice. Sensitive patient information does not have to be shared to be partners.

Law Enforcement Exception to Health Insurance Portability and Accountability Act (HIPAA)

'Medical personnel may not know the specifics of the law enforcement exception to HIPAA and may erroneously cite HIPAA as a reason for not proactively working with or seeking out law enforcement. But the law enforcement exception (45 CFR § 164.512(j)(1)(i), 2003)[164] allows for protected health information (PHI) to be reported to law enforcement to prevent or lessen a serious and imminent threat to the health or safety of an individual or the public. Additional information on under what circumstances a HIPAA-covered entity can disclose PHI to law enforcement can be found at http://www.hhs.gov/ocr/privacy.

The Importance of Integrating with Law Enforcement

A community approach to preventing terrorism and targeted violence is needed. Law enforcement alone cannot keep communities safe. Community members coming forward and working proactively with law enforcement allows for proactive mitigation options to occur, other than arresting individuals. Everyone benefits from decreased violence in communities. Consider revisiting your established threshold for law enforcement contact. In the past, the threshold for law enforcement contact was a criminal violation, meaning a crime had to be committed for law enforcement to be called. A cultural shift is needed where proactive prevention measures are implemented, rather than waiting for a crime to be committed. When concerns about mass violence occur, law enforcement should be called. Law enforcement officers are experts in public safety, but they cannot do their jobs if information related to concerning behaviors is not shared. Before a tragedy occurs, meet your local law enforcement members, seek out information about what BTAM resources are available in the area, and train together on what to look for related to preventing terrorism and targeted violence. Working proactively together allows our community partnerships to be built and fortified through community resources and partnerships.

164 U.S. Department of Health and Human Services (HHS); Office of Civil Rights [OCR]. (2003) Summary of the HIPAA Privacy Rule. Washington, DC: [Online]. Accessed: Summary of the HIPAA Privacy Rule | HHS.gov.

A Mental Health Perspective: Overcoming Barriers to Working Together With Law Enforcement

Kirk A. B. Newring, Ph.D.
Forensic Behavioral Health, Papillion, Neb.

Jessica Winternheimer
Magnolia Therapy and Consultation Services LLC, Omaha, Neb.

In many communities, a hospital or health care facility can be a nexus of community-based mental health providers, facility-based mental health providers and law enforcement officers, as each may play a role in the continuity of care with persons of concern (POC). In a behavioral threat assessment and management (BTAM) context, the more effectively behavioral health and law enforcement professionals can communicate, the more effectively BTAM professionals can work toward the shared goals of public safety and individual health and autonomy.

How a POC Arrives and Why It Matters

As described elsewhere in this work, targeted violence is often viewed as occurring as part of a continuum in which a person of concern has progressed on the pathway to targeted violence with a specific person, persons or place in mind. Some of the most common contexts include a current or former patient intending to harm a care provider, providers, employee or facility; a person engaging in targeted violence toward an employee for a reason unrelated to the setting (e.g., intimate partner violence intruding at the partner's workplace); or a family member or loved one with a grievance specific to an employee or group of employees following an adverse health care outcome. Within the hospital setting, the POC may "collect" additional grievances and shift their focus from one professional to another or expand to a growing number of potential targets. These examples have analogs in the corporate and educational BTAM environments.

Hospitals are often involved when a POC appears in need of emergency protective custody, psychiatric stabilization or inpatient care, and they can be involved in any lawsuit following an adverse outcome in which the hospital was directly or even tangentially involved. Unlike a school or business, a POC taken to the hospital may not be there voluntarily; moreover, a POC taken to the hospital is likely having one of their worst days to date, and any coping skills they attempted to deploy before the hospital visit likely led to law enforcement involvement and involuntary behavioral health care.

In nearly every community, a law enforcement officer may be the first professional a person experiencing a mental health crisis may encounter. After first contact, law enforcement or emergency medical specialists/technicians may be tasked with transporting the person to the health care facility where the "handoff" is to occur. Typically, these referrals originate due to concerns about suicidal ideation, perceived or expressed danger to others, or inability to care for oneself, leading to an emergency protective custody consideration. As discussed earlier in this work, the pathway to targeted violence begins with a grievance or a grudge. The initial obligation for the hospital is not related to threat assessment and management, though, as discussed below, it may become an obligation for the health care providers and the health care facility.

Behavioral Threat Assessment & Management: A Recap of *Tarasoff v. Regents of the University of California,* 1976

The Supreme Court of California issued their ruling in the case *Tarasoff v. Regents of University of California* on Dec. 23, 1974. In their lawsuit, the parents of Tatiana Tarasoff stated Poddar had disclosed an intent to kill a woman to his behavioral health provider, Lawrence Moore, Psy.D., who was employed by the Cowell Memorial Hospital at the University of California at Berkeley. Moore acted on this perceived threat Aug. 20, 1969.[165] Poddar murdered Tatiana

165 The interested reader can review additional information in open-source documents, including Mr. Poddar's criminal adjudication (10 CAL.3d 75O (1974) 518 P.2D 342 111CAL.RPTR. 910) the people, plaintiff and respondent, versus Prosenjit Poddar defendant and appellant, docket number criminal 16502.

Tarasoff on Oct. 27, 1969. Tatiana's parents sued both Moore and the university and asserted Tatiana's death was preventable given the information available to Moore. This case also highlights the role of the organization and facility in which the provider works: While the behavioral health provider was the focus of the lawsuit, so were the other involved professionals (law enforcement), as well as the hospital where behavioral health services occurred.

In the ruling, the court noted that a hospital must exercise reasonable care to control the behavior of a patient that may endanger others. The court also noted legislative steps that had been taken to protect good faith reporting by behavioral health providers who perceive a threat, citing California Evidence Code Section 1024: "There is no privilege under this article if the psychotherapist has reasonable cause to believe that the patient is in such mental or emotional condition as to be dangerous to himself or to the person or property of another and that disclosure of the communication is necessary to prevent the threatened danger." The court also noted that such disclosures are consistent with the ethical guides from the American Medical Association (AMA) at that time. The AMA noted that doctor and patient confidentiality can be pierced when "it becomes necessary in order to protect the welfare of the individual or the community." The court stated, "The protective privilege ends where the public peril begins."

While the case law is specific to California, many states and regulatory bodies have adopted *Tarasoff* guidance into practice. The reader is encouraged to identify the duty-to-warn obligations for facilities and included employees in their jurisdiction(s). In this section, we will use *Tarasoff* as a blanket term for the local governing legislation, case law, precedents and obligations related to the duty to warn (e.g., variance in terms such as "must," "shall" and "may.").

Tarasoff **and EMTALA in Practice**

The duty to warn or protect likely includes a behavioral health provider making a professional judgment on whether the person poses a threat, with that information then relayed as part of a civil commitment process. In practice, the duty to warn often includes asking law enforcement to complete a welfare check on the relevant parties, including the person that may pose a threat and the person or persons that may be in danger. Despite the window of 68 days between the assessment that Poddar posed a threat to Tatiana Tarasoff and her murder, the practical window appears to be somewhere between 24-72 hours for the initial obligation to stabilize the POC. A common experience is when the behavioral health client is referred for an emergency protective custody (EPC) assessment. Once in the hospital setting, if the patient states they do not have plans to harm anybody, or if they had thoughts of harming anybody but then promised not to act on those thoughts and to tell someone if the thoughts return, they may be discharged from an acute care setting as having achieved psychiatric stability as required by Emergency Medical Treatment and Labor Act of 1986 (EMTALA). Phrased differently, EMTALA requires that the POC be stabilized, while *Tarasoff* requires the threat of danger posed by the POC be reasonably addressed. The challenge for the provider, the BTAM team and the hospital is understanding and managing their obligations between the stabilization required under EMTALA and the duty to warn under *Tarasoff*.

Leaving the Hospital: What's Next?

While the ideal outcome is a satisfactory resolution of the health care concern with planned and coordinated follow-up care with a community-based provider, in many jurisdictions an initial EPC may expire after 72 hours if there has not been a determination that the person warrants a lengthier inpatient stay. This creates a potential context in which a person is released from care without a coordinated discharge plan. However, unless there is an EPC or other legal hold (e.g., civil petition), persons can leave against medical advice (AMA); again, they may be stable in accordance with EMTALA, though their potential dangerousness to others may be unaddressed.

No matter the manner in which the POC achieved discharge, the hospital BTAM team may have an obligation to share information with law enforcement and community-based health care providers in accordance with *Tarasoff*. If the POC's health care provider has a reasonable belief that the person who left AMA continues to pose a threat to themselves or others, they are obligated to follow their governing ethical and legal obligations related to duty to warn, protect, or warn and protect, at which point law enforcement may be contacted. At the agency or hospital level, the employees may need additional information about their local protections for making a good faith report to law enforcement. As noted above, typically the right to privacy ends when public peril begins.

Barriers to Effective Communication Between Mental Health Providers and Law Enforcement Professionals

Both facility-based and community-based health care providers face unique challenges in the BTAM ecosystem, including:

- Incomplete understanding of ethical obligations to client, community or both
- Incomplete understanding of legal obligations (when and to whom PHI can be shared)
- Incomplete understanding of good-faith reporting protections
- Concerns about scope of competence
- Insufficient training/low professional confidence in this context
- Low confidence in charting/billing for professional time
- Concerns about potential exposure to adverse licensure action
- Concerns about employment repercussions
- Concerns about potential damage to therapeutic rapport and relationship
- Low trust with law enforcement
- Lack of shared vocabulary (e.g., stable, threat, dangerous)
- Concerns that information shared will flow in only one way, with no integrated feedback process
- Concerns that what is legal may not seem ethical, and what is ethical may not seem legal, and sometimes what is ethical and what is legal are in direct conflict (i.e., reporting domestic violence between adults to law enforcement, while legally required, violates the social work ethical code of client/patient self-determination)

In discussions with colleagues regarding the assessment and management of threats made or threats posed, a common refrain is a concern about lack of qualifications and confidence in making decisions that impact assessment and management of threatening behaviors, and how that impacts the professional and their employer (e.g., feeling as though they have to "stay in their lane"). Additional concerns include a lack of clarity as to their individual obligations in terms of duty to protect, duty to notify, duty to warn and duty to safeguard others, which includes concerns about the limits of confidentiality and concerns about breaching confidentiality.

PHI, HIPAA and FERPA

The information provided above has identified and discussed some of the core components and misunderstandings related to protected health information (PHI) and, in some instances, concerns also relevant to educational records under the Family Educational Rights and Privacy Act (FERPA) (e.g., a counselor in an educational setting initiates an emergency protective custody act based on threats expressed by a client). With both HIPAA and FERPA, while there are protections for good faith reporting, providers or administrators unaware of the rights, responsibilities and protections under HIPAA and FERPA may hesitate to provide information to outside agencies such as law enforcement due to their misunderstanding of the obligations and protections under HIPAA, FERPA and other relevant legislation.

Integrating some of the themes above, therapists can have a potential fear that providing information to another will result in a one-way conversation in which the health care provider gives information about a patient or a party protected by the provider-client relationship while receiving no information from law enforcement about said patient. This experience or the fear of such an experience may be one of the more chilling factors impacting the willingness of behavioral health providers to share information with law enforcement in a context in which they are prevented from collaborating with law enforcement. The provider's agency may appreciate a benefit from front-loading education about this concern, noting that they may not hear back from law enforcement about the POC. It is an unfortunate reality that a client/POC who learns that a health provider made a good faith report to law enforcement may not want to return to that provider; indeed, many a behavioral health provider has been "fired" by their client after making a legal and appropriate contact with law enforcement about the client's safety.

Addressing Barriers Within the Hospital BTAM Context

A common refrain in trainings provided by threat assessment professionals is the benefit of highlighting the obligations and protections under HIPAA and FERPA as they speak to the provider of information, as those protections do not directly relate to the receiver of such information. Thus, in some contexts where a health care provider may have hesitancy in even identifying if a POC is a patient of theirs, law enforcement can help facilitate that discussion because HIPAA and FERPA do not prevent the law enforcement officer from giving information to that behavioral health provider, and (perhaps most importantly) communicating the urgency of the context. Phrased more directly, HIPAA covers the provider's mouth and hands as sources of information, but those laws do not address the provider's eyes and ears. Thus, should a clinician and a law enforcement professional find themselves needing to share information, the more information that law enforcement can provide to the clinician may assist the clinician in understanding how they can share confidential or protected PHI while minimizing any threats to the therapeutic relationship and/or licensure exposure and improving the client's quality of care. Should the law enforcement officer share their assessment that the client's welfare is an emergency, good faith reporting protections may apply (again, reporting protections vary by jurisdiction). HIPAA does not preclude a behavioral health care provider or hospital administrator from asking the law enforcement officer to help determine whether a law enforcement exception to HIPAA may apply if they view the current context as an emergency.

Information Sharing Among Mental Health and Law Enforcement Professionals Within a Hospital-based BTAM Context

Licensed health care providers may have access to no-cost legal consultation as a function of their membership in an organization or as part of their professional liability insurance. This provides an option for the provider to seek a consultation from a legal expert trained in confidentiality and sharing of information related to threats made and threats posed. The additional benefit is that the clinician can then document having sought consultation and guidance prior to making a call or deciding to not make a call. Providers who have used this method reported that the consultation helped clarify their thinking as to what information was relevant; what information, if any, needed to be shared; the best venue for sharing that information; and some of the self-protective steps that could be undertaken to assist the clinician in addressing some of the concerns mentioned above, such as licensure exposure, therapeutic rapport and a perceived one-way exchange of information.

The hospital or facility-based health care BTAM team is encouraged to provide proactive education, resources and ongoing guidance related to local laws and professional obligations as they relate to a duty to warn or protect persons, places or both.

Ideally, the POC is willing to sign necessary releases that allow for the exchange of PHI. While the POC can revoke consent at any time, should they provide consent to share PHI, the mental health care provider is encouraged to:

- Learn what information is to be shared.
- Learn the parameters of request for information (e.g., safety planning, investigation to inform an affidavit for a probable cause for arrest).
- Receive information that law enforcement provides.
- Document information received.
- Document receipt of signed release of PHI.
- Document to whom, when, and how the information was shared.

Recommendations Regarding Cooperation and Collaboration Among Mental Health and Law Enforcement Professionals

The enrollment numbers in the Association of Threat Assessment Professionals pale in comparison to the enrollment numbers in the American Psychological Association and American Psychiatric Association. Graduate training programs do not reliably include semester-long coursework on threat assessment. The practicum facet of training, including supervised practicum hours and internships, often addresses the *Tarasoff* concerns as professional development education or as part of a seminar or training event. These trainings typically will review indicators of elevated risk of suicide and indicators of elevated risk of homicide. As noted in the *Tarasoff* cases, one of the approaches to threat assessment was influenced by the aphorism, "The best predicator of future behavior is past behavior." Such a conceptual framework would compel one to conclude if a person has never murdered before then they will never murder, but a person who has murdered before may murder again. The data on homicide is quite the opposite; those who commit murder tend to commit *one* murder. Threat assessment and threat management approaches have identified several relevant precursors to targeted violence, with outpatient behavioral health providers often in a place where they may be the first to hear some of these private thoughts and risk indicators. The therapist's challenge then becomes receiving the patient's information, making an appraisal about risk of harm to the patient or others, and then fulfilling their obligations to warn, protect or both warn and protect. Should the behavioral health provider lack familiarity with behaviors of concern consistent with progression on the pathway toward targeted violence, the facility-based threat assessment team may be of assistance in eliciting the relevant information from the colleague that is unfamiliar with the terms and concepts, yet still a holder of vital information.

Potential action steps for the threat assessment and threat management teams within a health care system include creating a conceptual flowchart covering EMTALA and *Tarasoff;* clear and up-to-date guidelines on sharing protected health information within a BTAM context; bidirectional relationships with care providers in the community; and relationships with law enforcement, area schools and mental health crisis centers developed in advance of the need to make use of that relationship.

Adopting a continuing education program in conjunction with the hospital's or health system's legal department can be helpful in developing and sharing resources relating to PHI, mental health care and law enforcement, and, when open to community providers, in building bridges with local partners. For example, consider collaborative training efforts in which community health care providers, facility-based health care providers (such as emergency department or inpatient psychiatric units), legal community professionals, and law enforcement review and discuss how each group can play a role in the assessment and management of targeted violence, with each party becoming more familiar with the ethical duties and obligations for those vocations, and the limits of confidentiality and privacy within the context of threat assessment and management.

Bystanders: An Overlooked Resource

Christopher Desrosiers
Special Agent, United States Capitol Police
Task Force Officer, FBI BAU-1

The identification of potential behaviors of concern is the most critical and most challenging part of the behavioral threat assessment and management (BTAM) process. It not only requires that observable behaviors of concern be present, but also that bystanders are able to observe those behaviors, recognize them as concerning in some manner and report their observations to someone in a position to take further action.

Time and time again, research into attacks that were prevented credited bystander reporting as the factor that allowed for the opportunity for intervention to occur. In the hospital system, medical personnel, support staff, police, fire, EMS, patients and visitors can be key bystanders, as they all have the opportunity to directly observe behaviors in a variety of settings over a period of time. First responders and medical providers may also have access to key patient bystanders — friends, family, or other caregiverswho accompany the patient when medical care is being rendered. This direct contact with a patient bystander allows for direct questioning about behaviors observed during medical appointments. Hospital BTAM teams may harness potentially robust sources of information through the creation of a streamlined reporting process that is tailored to connect with these bystander groups. To facilitate the use of this process, BTAM teams can provide resources and training that encourage reporting and create a culture of shared responsibility in the prevention of violence within the health care community. This can be in the form of staff training, educational materials accessible to hospital patients and visitors, and BTAM program information shared with entities that have contact with the health care facility.

Recognizing that there are barriers to reporting that can include potential mistrust of the system, lack of knowledge of reporting mechanisms, lack of knowledge of what to report and fear of retaliation from the person of concern, all interactions with bystanders should be transparent and informative. These interactions should convey appreciation for their reporting and acknowledgement of their concerns. Reporting mechanisms (voice/text tip lines, emails, online portals, etc.) should also be designed to link multiple reports on an individual, as personnel or patients may move from one facility to another through their employment or medical care. These reporting mechanisms should also allow reports to be received even if the person of concern is not a patient or employee. This continuity in health care BTAM operations will help to ensure that all bystander reporting is acknowledged and reviewed, and individuals of concern do not slip through the cracks. A system that is accessible and reliable for bystanders will allow them to become a critical BTAM force multiplier in health care violence prevention efforts.

Don’t Forget EMS and Fire: The Importance of Nontraditional Partners in BTAM

Heather M. Koch
Supervisory Special Agent, FBI

In 2023, there were more than 54 million emergency medical service (EMS) activations in the United States involving over 14,000 agencies. Of these activations, more than 36 million calls for service resulted in the treatment and/or transport of patients to medical facilities.[166] Traditionally, dispatchers, fire departments and EMS have been on the front lines of calls for pre-hospital service and are often the first to assess a multitude of factors surrounding patients, the environments from which they came and the behaviors they and those around them exhibit. As such, those involved in pre-hospital care should be considered vital partners in behavioral threat assessment and management (BTAM) efforts.

Identifying potential concerns often begins with dispatchers. Dispatchers are uniquely positioned to evoke information from callers, including reported concerning behaviors. Dispatchers can also evaluate call history related to the patient(s) and/or their location to identify and assess possible escalating behaviors. Making dispatchers aware of what might constitute concerning behavior can help ensure appropriate follow-up questions are asked and information is relayed to responders. With this information, responders can conduct more focused questioning of patients. Certain types of calls may naturally suggest larger possible BTAM concerns. Suicide attempts or ideation, mental health crises, injuries associated with domestic violence, or calls related to ongoing issues with chronic or terminal health concerns are several examples of situations that could present or lead to grievances that have the potential to involve health care workers and/or the facilities where they work. The ability to observe the patient’s environment and their interactions with others should be noted and discussed with receiving facilities.

Assessing a scene for potential risks, or “scene size-up,” is fundamental to ensuring a safe operating environment for emergency medical providers, the patient and bystanders. First responders initiate scene size-up well before patient contact is made. The amount of time EMS providers spend on scene and during patient transport is usually rather limited. As such, pre-hospital providers’ ability to obtain comprehensive patient histories inclusive of environmental and circumstantial factors is vital to ensuring receiving facilities are aware of potential risks not only for affective violence but also potential targeted violence directed at those facilities and their providers. EMS providers are adept at assessing patient cognition, performing trauma assessments and eliciting medical histories, and are also highly practiced at observing and assessing those environments from which patients are transported.

Moreover, ensuring information is relayed between alternating crews within fire departments and EMS agencies is important. Many fire departments operate on 24-hour cycles; allotting time during shift handoffs to ensure incoming crews are aware of patients, or people associated with patients, who have demonstrated concerning behaviors or who have made concerning statements should be considered a best practice. Pre-hospital responders may be in a position to receive information related to concerning behaviors exhibited by patients and/or those associated with them; they, too, should be prepared to relay that information to the appropriate parties. Responders should also be aware of statements made by patients, patients’ families, etc., in the pre-hospital setting that may suggest discontent or a propensity for violence directed toward specific facilities or providers. Routine communication and information sharing between pre-hospital providers can help identify instances where concerning behaviors may be escalating from thought to possible action. In turn, receiving facilities should ensure when accepting patients from pre-hospital providers that they not only obtain the patient’s medical history but also understand the context/environment from which the patient came. In summary, dispatchers, fire and EMS personnel possess unique, and sometimes cumulative, insight on patients who ultimately end up in hospital systems, and they should be considered vital partners in BTAM efforts.

---

166 National EMS Information System (NEMSIS), (2024) NHTSA Office of Ems, Department of Transportation, 2023 Data Report.

Author Bios

- **Christopher Desrosiers** is a special agent with the United States Capitol Police (USCP). He began his law enforcement career in 2007, serving in the department's Uniformed Services Bureau before joining the Investigations Division in 2013. Since that time, S/A Desrosiers has been assigned to USCP's Threat Assessment Section (TAS). In addition to his investigative duties, S/A Desrosiers is a field training agent, a member of TAS' Behavioral Sciences Group, and an adjunct instructor at the USCP Training Academy across the multiple training programs that serve the department's Protective Services Bureau. S/A Desrosiers also serves as a task force officer at the FBI's Behavioral Analysis Unit within the Behavioral Threat Assessment Center.
- **Robert Fein, Ph.D.,** is a forensic and national security psychologist with a specialty in threat assessment and the prevention of targeted violence. For over 40 years he has worked with law enforcement and intelligence organizations to understand and prevent targeted violence such as assassination, workplace violence, stalking, school violence and terrorist attacks. Since 2015, Dr. Fein has served as a consultant to the FBI's Behavioral Analysis Unit-1 and to the FBI's Behavioral Assessment Program. In that capacity he consults on counterintelligence, counterterrorism, threat assessment and prevention of targeted violence cases.
- **Karie A. Gibson, Psy.D.,** is a licensed psychologist and has been a special agent with the FBI for over 19 years, currently serving as the unit chief for the FBI's Behavioral Analysis Unit-1 (BAU-1) Behavioral Threat Assessment Center (BTAC). BTAC is a national-level, multi-agency, multidisciplinary task force focused on the prevention of terrorism and targeted violence through the application of behaviorally based operational support, training and research for local, state, federal and international partners. BTAC routinely completes threat assessments, threat management strategies, statement analysis, interview and interrogation strategies, prosecutorial strategies, media strategies, and unknown offender profiles. Dr. Gibson served as a supervisory special agent/profiler at BAU-1 for nearly seven years prior to being promoted to unit chief in 2021.
- **Angel Gray, J.D., MPH, CTM,** is the director of threat assessment and management at the University of North Carolina at Chapel Hill, where she leads campus-wide efforts to prevent and respond to behavioral threats. Prior to joining UNC in 2023, she was the general counsel for the North Carolina State Bureau of Investigation, where she co-founded North Carolina's first Behavioral Threat Assessment Unit, known as BeTA. She also served as legal advisor to the North Carolina Department of Health and Human Services, providing counsel on hospital operations and health care licensure, and was an adjunct instructor for the UNC-Chapel Hill Forensic Psychiatry Fellowship Program. She is a member of the Association of Threat Assessment Professionals and a certified threat manager.
- **Nicole Tuomi Jones, Ph.D., CTM,** is a licensed psychologist with the Behavioral Threat Assessment (BeTA) Unit of the North Carolina State Bureau of Investigation. For over two decades, Dr. Jones has combined clinical expertise with operational practice, specializing in the behavioral assessment of individuals with serious mental illness and serious emotional dysregulation. Since joining BeTA in 2018, Dr. Jones has been involved in more than 400 threat assessment cases, led research-to-practice initiatives to bridge the gap between psychology and law enforcement, and developed the North Carolina BeTA Investigation Overview — known as NCBIO-25 — a structured professional judgment tool created to support law enforcement in behavioral threat assessment and management cases. Dr. Jones is a member of the Association of Threat Assessment Professionals and a certified threat manager.
- **Heather M. Koch, MPS,** is an FBI Supervisory Special Agent (SSA) currently assigned to the Tampa Field Office. Previously, SSA Koch was a profiler at the Behavioral Threat Assessment Center/Behavioral Analysis Unit-1. SSA Koch entered on duty with the FBI in 2007 after serving four years as a deputy United States marshal. SSA Koch has also spent time in the FBI's New Orleans, Los Angeles and Miami field offices in addition to serving two tours at FBI headquarters. Prior to joining the U..S Marshal Service, SSA Koch worked as a certified firefighter/emergency medical technician (EMT) in central Florida. SSA Koch has maintained EMT licensure since 2001 and has remained an active participant in the FBI's Operational Medicine program. In 2020, SSA Koch earned a master's degree in emergency and disaster management from Georgetown University.

- **Ed Markowski, MA, LPC, CTM,** is the director of threat assessment at the University of Virginia. Over his 17-year threat assessment career within higher education and health care industries, he has assessed, managed and consulted on thousands of cases involving communicated threats, weapons, intimate partner violence and stalking. He is a licensed professional counselor, a member of the Association of Threat Assessment Professionals, a certified threat manager and a Department of Homeland Security certified master trainer in behavioral threat assessment.

- **Andrew Muck, M.D., MBA,** is a physician and former U.S. military officer who has built his career at the intersection of emergency medicine, leadership and preparedness. He has served on the faculty at UT Health San Antonio before becoming chair and professor of emergency medicine at the University of Virginia, where he holds the Marcus L. Martin Distinguished Professorship and leads the department's academic, research and clinical missions. His work with the Critical Incident Analysis Group focuses on advancing operational readiness, innovation and system-level solutions to complex challenges in health care and security through community shielding. Drawing on military service and leadership in two major academic medical centers, he brings a unique perspective on resilience, crisis response and collaborative problem solving.

- **Kirk A. B. Newring, Ph.D., CTM,** is a licensed clinical psychologist in the states of Nebraska, Iowa, Kansas, Washington and New Mexico, and maintains an interjurisdictional credential that allows for the practice of telepsychology in over 40 states. He maintains a private practice near Omaha, Neb., focusing on forensic mental health. His work has included fitness assessments for licensure boards, law enforcement agencies and health care organizations. He has provided instruction for undergraduate and graduate students, as well as psychiatry residents. Dr. Newring has contributed to the field with a number of publications and has presented at local, national and international conferences and continuing education events. In addition to a number of courts-martial, Dr. Newring has provided expert witness testimony in more than 150 cases in state courts and federal courts in Texas, Iowa, Nebraska, South Dakota and New Mexico.

- **Susannah Rowe, M.D., MPH, FACS,** has served as faculty in the Department of Ophthalmology of the Boston University Chobanian & Avedisian School of Medicine for over 25 years. In her role as associate chief medical officer for wellness and professional vitality at Boston Medical Center, she leads institutional efforts to improve occupational equity and well-being, focusing on local and national drivers and the particular experience of highly mission-driven clinicians. Throughout her academic and clinical career, Dr. Rowe has been driven by a deep commitment to fostering environments — both individual and institutional — that enable people to thrive.

- **John "Jack" Rozel, M.D., MSL, DFAPA,** is the clinical chief of crisis services at UPMC Western Behavioral Health and the co-director of the UPMC Systemwide Threat Assessment and Response Team. He divides his time between violence work and emergency psychiatry and is a past president of the American Association for Emergency Psychiatry. Dr. Rozel is a professor of psychiatry and aw at the University of Pittsburgh and is board certified in general, child and forensic psychiatry. He teaches and consults with teams across the country on behavioral threat assessment and management and workplace violence prevention.

- **Gregory Saathoff, M.D.,** is the forensic psychiatrist for the FBI's Behavioral Analysis Unit-1 and a professor of emergency medicine and public health sciences at the University of Virginia's School of Medicine.

- **Mario J. Scalora, Ph.D.,** currently leads the Targeted Violence Research Team at the University of Nebraska-Lincoln, supervising research regarding a range of issues related to the assessment and management of targeted violence. His research and consultation facilitate the implementation of evidence-supported practices at the agency, institutional and community levels. Dr. Scalora has an extensive background as a practitioner and consultant to various law enforcement, educational and human service agencies at the local, state and federal levels. He and colleagues at the University of Nebraska Public Policy Center continue to assist with developing threat assessment and management activities across an array of agencies and facilities.

- **Melissa Stormer, Psy.D.,** is a supervisory special agent with the Office of Special Investigations (OSI) and a clinical/forensic psychologist. She has been an OSI agent for 21 years and has experience working and advising on investigations regarding violent crimes, sex crimes, crimes against children and national security matters. Her education and experience have focused on serious mental illness, personality disorders, sexual deviancy and predatory behavior. Dr. Stormer also conducts court-ordered evaluations regarding violence risk, sexual risk, competency to stand trial and mental status at the time of the offense for the Commonwealth of Virginia. She was assigned to the FBI's Behavioral Analysis Unit-1 in February 2022.

- **Jennifer Tillman, MA,** is a crime analyst assigned to the FBI's Behavioral Analysis Unit-1 Behavioral Threat Assessment Center. CA Tillman works alongside special agents providing behavioral-based operational and analytical support on counterterrorism and threat prevention cases. During her 18-year tenure, she has testified to her products during grand jury proceedings and trials. She has worked on a myriad of post-attack investigations and provided threat assessment and threat management training across the country. She was the recipient of the FBI Medal of Excellence in 2021.

- **Lynn Van Male, Ph.D., CTM,** is the senior director of threat management for Kaiser Permanente National Security Services, the past national director of the U.S. Veterans Health Administration's Workplace Violence Prevention Program (2011-2023), a past second vice president of the Association of Threat Assessment Professionals (2017-2021), and an assistant clinical professor of psychology at Oregon Health & Science University. She is president and sole proprietor of Lynn Van Male, LLC, a private consulting firm. Predating her executive leadership positions, Dr. Van Male delivered over 20,000 clinical contact hours of direct patient care services focused on post-traumatic stress disorder recovery.

- **Jessica Winternheimer, MSW, MSOL, LICSW,** is a licensed independent clinical social worker with over 20 years of experience in behavioral health. She is the owner of Magnolia Therapy and Consultation Services, where she provides therapy for women navigating anxiety, depression, trauma and life transitions, as well as consults for threat assessment and crisis response. She is a certified clinical trauma professional and former certified threat manager. She has extensive experience in medical settings and private practice.