SIW SECURITY INFOWATCH.COM

SECURITY EXECUTIVES

Trends in Healthcare Clinic Security

It is critical to take a strategic approach to creating a security roadmap for healthcare facilities to mitigate risk and stay compliant

Frank Pisciotta, Bryan Warren, CHPA,CPO-I

The rising violence in healthcare facilities is not limited to hospitals. Clinics that are not physically attached to a hospital or on the same campus do not typically have the same level of protection and security staffing as a hospital. Furthermore, larger health systems may have hundreds of these facilities that need to be considered, and these facilities are not without risk. Security staffing, technology deployment, and training at these clinics may not be as robust as they are at acute care facilities.

Examples of incidents involving loss of life in clinic settings include:

- Northside Medical Midtown Laureate Medical Group, Atlanta
- Ambulatory Surgery Center Francis Health System Natalie Building, Tulsa, OK
- Allina Health Clinic Allina Health Buffalo, Buffalo, MN
- Orthopedic and Physical Medicine Associates, Rancho Mirage, CA

Such loss of life events garner significant media attention, but the day-in and day-out issues at these clinics are verbal abuse and physical violence. Some clinics have traditionally provided higher-risk services and some characteristics must be considered:

- Types of services being offered (e.g., behavioral health, chemical dependency)
- Hours of operation (e.g., weekends and night hours)
- Crime and neighborhood characteristics (e.g., is the clinic located in an area where other facilities may attract criminals to the area)
- Presence of narcotics and medications (outpatient pharmacies, pain management services)
- Response time of security or local law enforcement if an incident were to occur.

The major challenge for healthcare administrators and security leadership is to determine how to allocate limited financial resources to provide a reasonable level of security to a variety of facilities where the security incident experience may range from infrequent and unpredictable to routine and high risk.

Here are five strategies available to clinics to overcome these challenges:

1. Develop a methodology to prioritize clinics from a security perspective to determine a strategy for the allocation of security personnel (e.g., full-time, patrols only, "as needed").
2. Enhance the security of a site using remote monitoring from centralized control locations.

3. Establish technical security standards to ensure that risks identified are mitigated uniformly in new construction or renovations.
4. Train clinic staff on workplace violence detection and prevention, the location and use of security technology (panic buttons, access controls), and how and when to contact local law enforcement for assistance.
5. Conducting a Security Risk Assessment (SRA) with a qualified healthcare security professional* to determine the adequacy of current security measures and identify opportunities for improvement.

Security Staffing

As mentioned previously, many clinic and outpatient facilities may suffer from security incidents; however, such events may be so infrequent as to preclude the need for a full-time security presence at the facility. Having security personnel posted at a facility with little or nothing to do is not only inefficient from a resource perspective but can also lead to a host of problems including performance issues and unprofessional behaviors (e.g., sleeping on the job, use of personal phones and the appearance of inattentiveness which reflects poorly on the security department). One method to identify a staffing model for such areas is to use an objective process that considers appropriate criteria. Such criteria should include not only the items mentioned earlier (e.g., size of the clinic, types of patient populations served, hours of operation, area crime statistics) but also a review of key metrics and performance indicators (KPIs) regarding the security function (e.g., alignment with clinical leadership on acceptable security response times).

> *“The major challenge for healthcare administrators and security leadership is to determine how to allocate limited financial resources.”*

BPS and some healthcare organizations have developed algorithms to rank order and collect data to determine staffing (and technology) strategies for clinics. We encourage all health systems to take this step.

Recognizing security trends, especially those that may result in adverse impacts to staff or patient safety, may seem like a simple proposition; however, to translate the true importance one must be able to speak in a language that administrators will understand. This is where metrics and KPIs can assist since many healthcare leaders have backgrounds in business rather than medicine. If you can establish an issue by using data and demonstrate negative impacts to the organization if the trend continues (by predicting outcomes should no action be taken), then you may have a much better chance of getting and keeping the attention of those with the authority to commit resources.

One can likewise project what the real cost (in potential injury claims and compensation) and potential cost (in possible litigation or regulatory penalties) could be should the issue remain unresolved and compare this to the cost of security personnel (either full-time, part-time or as a shared expense between multiple sites as a regional patrol position). By translating metrics into real-world dollars and cents, you can better establish a preventative Return on Investment (ROI) to resolve the issue. As the old saying goes, the numbers do not lie (assuming you have good data).

Remote Monitoring

Should calculations indicate that a full-time security presence is not reasonable for a particular site, then the use of security technology as a force multiplier should be considered. Many clinics and outpatient sites already use after-hours alarm systems to detect unauthorized entry attempts when the building is not open for patient care. Using "real-time" remote monitoring of duress or panic alarms, video surveillance feeds, and the ability to quickly restrict access into a facility from an offsite operations center should a credible threat take place, the security of a clinic can be significantly enhanced.

The use of such a centralized model offers many advantages including the speed in responding to security events, consistency of preventive maintenance of security systems and equipment and the ability to provide such services regardless of the clinic's location or hours of operation. A critical aspect of using remote monitoring services is the creation of technical standards for the selection, installation, and operation of security-related technology to provide uniformity in the mitigation of potential threats.

Technical Security Standards

There are two facets to establishing technical security standards. The *first* is defining the physical security performance requirement of physical and technical security in the clinic setting. Performance standards may be applied in a layered concept for clinic settings.

- Layer one area would be between the property boundary and the building perimeter. The layer one space may or may not be controlled and restricted based on the level of crime around the clinic.
- Layer two spaces would be considered areas of the clinic where the facility is freely accessible. This may include visitor and patient reception areas and in some cases areas where delivery drivers may be allowed to enter to coordinate deliveries and pickups (e.g., lab functions).
- Layer three spaces are for staff and patients only and would typically be access-controlled to prevent free entry.
- Layer four spaces would be restricted areas such as server rooms or medication storage areas.
- Layer five spaces would include secure containers within restricted areas that may house protected health information (PHI) or narcotics/pain medications necessitating stricter controls for access and dispensing.

Performance standards can be established for each of the areas above based on the unique characteristics of the clinic and how access is limited when moving from one security area to the next.

> *"When standards exist, it can reduce training expenses. Supporting fewer equipment varieties lowers the investment required for training technicians, operators, and end-users."*

The *second* element of technical security standards relates to establishing physical security equipment standards which can enhance consistency across all facilities. For example, personnel who may work at different clinics do not have to get accustomed to different duress alarm devices from one location to the next. Additionally, standard equipment can save money by reducing the number of software platforms and server applications necessary to support common systems (e.g., access control and video surveillance). For larger organizations that may maintain their technical installation and maintenance resources, standardization simplifies maintenance and support and allows staff to become familiar with specific equipment models, making it easier to troubleshoot and maintain inventory of spare parts.

When standards exist, it can reduce training expenses. Supporting fewer equipment varieties lowers the investment required for training technicians, operators, and end-users. Proper vetting at the front end will avoid decentralized purchasing practices that can run afoul of the National Defense Authorization Act (NDAA) when sites try and cut corners for cost savings.

Staff Training

While security technology and associated systems are a tremendous resource when implemented properly, there is still the issue of education and training of staff working in the environment that is being protected. Workplace violence rates in healthcare continue to increase in the U.S., and outpatient and clinic settings are no exception. In addition to workplace violence prevention training programs (which are required based upon several regulatory and accreditation agencies), staff working in offsite or remote locations should also be routinely educated on the types of security measures in place at their facility, how these devices function, and when they should be used.

A panic button is ineffective if clinic staff do not know where it is or how to operate it during a stressful event, and the same is true for other security measures such as the identification and location of safe rooms should an active assailant event occur. Other security-related topics that should be considered for these workers include personal safety and situational awareness, crime prevention, and conflict resolution techniques. How can you determine if your security measures and staff education and training efforts are adequate?

Security Risk Assessments

There are a lot of factors which vary from clinic to clinic. There is no substitute for the sound practice of executing a security risk assessment. There are three significant drivers for this action:

- ***OSHA General Duty Clause 5 (a) 1*** which requires an employer to furnish to its employees: "employment and a place of employment which are free from recognized hazards that are causing or are likely to cause death or serious physical harm to his employees..."
- ***Tort Law Premises Liability*** which is a legal doctrine under which the owner or occupier of a property can be held financially responsible for torts (violent crimes) that occur on their premises.
- ***International Association of Healthcare Safety and Security (IAHSS) Guideline 01.04 Security Vulnerability Assessments***. The IAHSS calls for this assessment to evaluate if the program is susceptible to

any known weaknesses or risks, assigns severity levels to those vulnerabilities, and recommends remediation or mitigation if needed. Security Vulnerability Assessments should be conducted by a qualified healthcare security professional on a regular ongoing basis or when the environment changes.

The failure to take this crucial step can open an organization to fines, damage to the brand and liability.

Summary

There are challenges when it comes to determining appropriate security measures for clinics and other standalone healthcare facilities. The authors provided five strategies to overcome the unique challenges associated with healthcare clinics:

1. Develop an algorithm and key performance indicators to determine when and how to provide security staffing to mitigate identified risks.
2. Enhance the security of a site using remote monitoring from centralized control locations.
3. Establish technical security standards to ensure that risks identified are mitigated uniformly in new construction or renovations.
4. Train of clinic staff to include workplace violence detection and prevention and the location and use of security technology (panic buttons, access controls).
5. Conduct a Security Risk Assessment (SRA) with a qualified healthcare security professional to determine the adequacy of current security measures and identify opportunities for improvement.

Bryan Warren, MBA, CHPA, CPO-I is President and chief consultant at WarSec Security.

Bryan Warren, MBA, CHPA, CPO-I *is President and chief consultant at WarSec Security and has more than 33 years in the healthcare security, safety and emergency management fields. He has conducted healthcare security assessments and training workshops across the United States, Canada, Europe and Australia and holds a bachelor's degree in criminal justice and an MBA with a focus on legal foundations of healthcare. Bryan is a Certified Healthcare Protection Administrator as well as a Certified Protection Officer Instructor and has served on several national task forces including the U.S. Centers for Disease Control and the Department of Health and*

Human Services Office of Infrastructure Protection. Bryan is a Past President of the International Association for Healthcare Security and Safety (IAHSS), providing presentations nationally and internationally on the healthcare environment.

Frank Pisciotta is president of Business Protection Specialists, Inc.,

Frank Pisciotta is president of Business Protection Specialists, Inc.*, a nationwide independent physical security consulting firm focused on risk assessment and security design services including the specification of technical solutions in a wide array of industry sectors. Frank Pisciotta has managed over 5,000 security-consulting engagements in his more than thirty-three-year consulting career. Frank possesses a master's degree in public administration, and a bachelor's degree in criminal justice, and was board-certified in Security Management by the American Society for Industrial Security as a Certified Protection Professional in 1994. He is a past President of the International Association of Professional Security Consultants. Frank was the eighth person in the United States to achieve the Certified Security Consultant designation.*

* Qualified healthcare security professional: standing, or skill, and who, by knowledge, training, and experience, has demonstrated the ability to perform the work. A qualified healthcare security professional may be a Certified Healthcare Protection Administrator or one with healthcare-specific security expertise and certification such as a Certified CPTED Practitioner or Certified Protection Professional with healthcare-specific security expertise.

Source URL: https://www.securityinfowatch.com/security-executives/article/53097035/trends-in-healthcare-clinic-security