FINDINGS

SECURITY:
Mitigating Risk in Healthcare Facility Design

A Module on a Safety Risk Assessment Component

THIS SAFETY MODULE INCLUDES:

Backgrounder
Design Strategies
Issue Brief

This module was created as a supplement to the Safety Risk Assessment (SRA) toolkit and other SRA-related Issue Briefs, Backgrounders, and Top Design Strategies. This toolkit is not intended to be a guarantee of a safe environment; the environment is one part of a safety solution that includes operational policies, procedures and behavior of people. It is intended for use with collaborative input of project- and facility-based expertise.

The Safety toolbox is made available through a partnership with Grainger.

This document will be updated in 2018 to be a stand-alone reference under the Grainger sponsorship.
Understanding Security and Risk


Certain patient populations are more at risk than others from a security and elopement perspective. Areas such as the infant birthing center are at a security risk for kidnapping, while in other areas, such as behavioral health, patients may be at risk for elopement (i.e., wandering/running away or escaping prior to scheduled discharge). Assessing the security/elopement vulnerability of each patient population will help establish the consequent requirements in the physical environment. Security-sensitive patient areas should be identified by taking into account the risk that particular patient conditions in the unit pose to elopement/security breach.

A comprehensive written security plan should be developed for normal and contingent operations to address the overall site, individual buildings, and all security-sensitive areas (as relevant to the scope of the project). The plan should take a layered approach to access control, including (but not limited to) security-sensitive zones, control points, circulation routes, and required egress paths, and should consider any impact relative to existing institutional security plans.

It is essential to identify areas requiring the segregation of authorized and unauthorized persons and areas requiring the segregation of the public, patients, and staff to determine the level of security as well as suitable security measures. Highly sensitive areas are limited to vetted and authorized staff and should be addressed alongside regulatory oversight, standards, and guidelines, as each area may have specific concerns. Such areas often include the pharmacy and other storage spaces for narcotics; areas containing hazardous material; plant utility and information technology infrastructure; and areas housing personal health information.

During the overall planning of the project, it is also important to think about the security risk to the healthcare facility “during” construction. This can be a threat not
just to property, but also, in the case of renovation projects, to the existing patients and staff. A security plan for the construction phase should be developed that is risk-appropriate for both the environment and function of the project space. This includes:

- A description of the impact of demolition and phasing on existing site functions, as well as protection strategies and design interventions;
- An assessment of the need for temporary security barriers such as fencing and security systems, including intrusion detection and video surveillance; and
- A schedule for installation of security systems for completion during early move-in activities to allow for protection of the facility and equipment.

Security considerations also include protection at the perimeter of the property, at the building perimeter, and inside the building. A clear understanding of the different points of access; circulation routes; patient, visitor, staff, and administration zones; and egress routes for regular and emergent situations is necessary before putting security measures into place. Considering all vulnerabilities at an overall planning/policy level can help to create a safe and secure environment.

Security incidents may cause actual harm to patients, families, and staff on various severity levels ranging from minor injuries to injuries or harm requiring medical treatment, as well as disabilities or sentinel events. It is important to evaluate the likelihood and severity of the probable harm caused by security incidents in various areas of a facility, including the highly sensitive areas, at early design stages. A clear understanding of areas which require the segregation of authorized and non-authorized personnel is also important. This will help to focus efforts on those security issues that may cause the most harm.

References

OVERVIEW

Designs to mitigate the risk of security breaches include considerations for integration with outside agencies as well as systems within the facility. Controlling access and maximizing visibility throughout the site, parking lot, building entrances, and interior are key considerations that need to be balanced with needs for privacy.

Safety Risk Assessment: Security Design Strategies

The following design solutions are a brief summary of the content found in the SRA Issue Brief “Security: Mitigating Risk in Healthcare Facility Design.” They are organized by building design category.

Site Optimization

- Address the organization’s role in using the facility to respond to internal and external emergencies. (This may be on its own, or in coordination with local emergency response or public health authorities based on the assessed risk.)
- Identify controllable entry points to the campus for emergency/heightened security situations, and limit and control points of entry into the site (both vehicular and pedestrian).
- Provide adequate and unobstructed lighting to enable surveillance of the grounds surrounding a healthcare facility. (This consideration is also related to lighting.)
- Avoid or eliminate places of potential concealment or habitation in the landscape, and maximize visibility (i.e., provide unobstructed sightlines).
- Design parking facilities according to specific security considerations, including: limitation/control of entries/exits, protective lighting, physical protective barriers, and video surveillance. To maximize the visibility of activity, position attendant booths, parking offices, or security stations (if used) where attendants/officers can directly monitor activity in the parking area and maximize the line of sight into areas of the parking lot. Avoid or eliminate dead-end parking areas and areas of concealment.

Technology Integration

- Provide an emergency radio communication system in each facility that operates independently of the building’s service and emergency power systems and allows direct communication with security, law enforcement, or other mechanisms to obtain immediate assistance.
- Consider a single unified or integrated system for access control, video surveillance and, when appropriate, parking access and egress, debit card functions, and time and attendance needs.
• Enable the security system to completely shut down vehicular and pedestrian access if needed.

**Building Layout**

• Locate security officer posts and/or police officer workstations (when accommodated in a building) to maximize visibility at public entrances, waiting areas, registration, and information areas.

• Limit and control points of entry and exit to/from the building, while ensuring vehicular and pedestrian safety.

**Building Envelope/Structure**

• Put in place penetration-resistant protective measures that extend from solid floor to solid ceiling or roof in the building envelope for highly security-sensitive areas.

**Unit Layout**

• Implement segregation of authorized and unauthorized visitors in security-sensitive patient areas, and ensure that patient and visitor paths (or “screened public” paths) do not pass through designated staff-only security zones.

• In patient care areas where there is a high risk of physical violence to staff, design workstations to prevent unwanted access. (The degree of enclosure and protective material used should depend on the assessed vulnerability and patient population.)

• Position workstations in security-sensitive areas to provide staff direct access to an exit (a safe drop-back zone), and equip them with strategically located duress alarms.

• Install intrusion detection systems in high-risk areas of the hospital that are not staffed 24/7.

• Provide adequate and unobstructed electronic and natural surveillance where there may be aggressive or disruptive patients, while at the same time minimizing compromises in patient and staff privacy.

• Identify unique security risks presented by highly hazardous materials, including but not limited to biological, chemical, and radioactive materials.

• Use physical separation and other security measures to prevent unauthorized access to areas in healthcare facilities containing hazardous materials.
Interior Design/Finishes

- Ensure that wayfinding and other signs do not compromise direct visibility (sightlines) and electronic surveillance systems.

- Evaluate electronic security issues, and the safety and security of information systems, during the design of the physical environment to take into account necessary power and data.

Mechanical (HVAC)/Electrical

- Consider the protection of HVAC systems against chemical, biological, and radiological attacks (e.g., protection of outside air intakes, location of return air grilles, and types of filtration).

Department-Specific Considerations

Pharmacy Areas (Central or Satellite)

- Create a secure physical separation between pharmacy operations and the public using penetration-resistant protective measures that extend from solid floor to solid ceiling or roof, while maintaining clinical accessibility.

Room Layout

- Provide the following in all medication dispensing areas:
  - A secured room or area for reception, breakout, and inventory control of materials used in the pharmacy;
  - A secured area for temporary storage, exchange, and restocking of carts; and
  - Security provisions for drugs and personnel in the dispensing counter area.

- Prevent pharmacy access above suspended ceilings through air ducts, cable or utility infrastructure, roof hatches, skylights, unprotected external windows, doors, and dumbwaiters. (This consideration is also relevant under mechanical (HVAC)/electrical.) Also provide secured storage cabinets, shelves, and/or separate rooms or closets for the following, as required:
  - Volatile fluids and alcohol in accordance with applicable fire safety codes for the substances involved; and
  - Narcotics and controlled drugs.
Medical Records/Health Information Management Areas

- Locate medical records away from treatment and public areas, and/or restrict medical records to areas with staff access only.

- Secure medical records in all media (paper and electronic), and protect them from loss or damage as required by the functional program. (This is also related to category of unit layout, if paper medical records are used.)

Emergency Departments

- Ensure the ED cannot be accessed by unauthorized visitors or personnel at any time.

- Locate ED reception or triage areas to provide unobstructed and uninterrupted staff observation of public access points to the department, the public waiting area (including patients who are waiting for treatment), and the treatment area.

- Designate access-controlled and monitored (video and audio surveillance) patient/observation rooms for disruptive/aggressive patients or patients at high risk of elopement. (This is also related to the considerations for injury of behavioral health.)

- Include access to panic buttons for security emergencies in high-risk areas (e.g., triage).

Additional Resources


This summary was created as a supplement to the Safety Risk Assessment (SRA) toolkit and other SRA-related Issue Briefs, Backgrounders, and Top Design Strategies. This toolkit is not intended to be a guarantee of a safe environment; the environment is one part of a safety solution that includes operational policies, procedures and behavior of people. It is intended for use with collaborative input of project- and facility-based expertise.
FINDINGS

SECURITY: Mitigating Risk in Healthcare Facility Design
An Issue Brief on a Safety Risk Assessment Component

INSIDE YOU WILL LEARN ABOUT:

The integration of security considerations with emergency planning.
Layers of security protection.
Ways to enhance visibility through both natural surveillance and technology.

This issue brief was created as a supplement to the Safety Risk Assessment (SRA) toolkit and other SRA-related Issue Briefs, Backgrounders, and Top Design Strategies. This toolkit is not intended to be a guarantee of a safe environment; the environment is one part of a safety solution that includes operational policies, procedures and behavior of people. It is intended for use with collaborative input of project- and facility-based expertise.
In the context of preventing harm and loss in healthcare settings, there is a relationship between safety and security. Safety is often associated with accidents (inadvertent harm), whereas security is often associated with a conscious decision or intent to cause harm (York & MacAlister, 2015). However, since accidents and disasters are both security-related events, security concerns can be seen as spanning a range from intentional harm (e.g., burglary, arson) to unintentional harm (e.g., natural or man-made disasters, accidental fire).

In the context of the National Quality Forum’s “never events,” security is aligned with patient protection associated with suicide, elopement, and/or criminal acts, such as abduction or serious injury from assault. Layers of protection (IAHSS, 2012) should be incorporated to offer protection:

- At the perimeter of the facility site;
- At the building perimeter;
- Against unauthorized visitor access to security-sensitive areas;
- Against unauthorized access to non-public areas of the healthcare facility; and
- Against unauthorized staff access to highly sensitive areas.

Conditions that contribute to improved security include physical controls, psychological deterrents, and often an interaction between the two (York & MacAlister, 2015). Latent (underlying) conditions include:

- Control of access points into the site and at the facility perimeter;
- Lighting of the site and parking;
Building Envelope:
A second layer of protection occurs at the building perimeter, where access to doors, windows, and other openings is controlled, especially in security-sensitive areas.

- Visibility to provide direct lines of sight and surveillance both inside and outside;
- Adjacency of security-sensitive areas (e.g., intensive care, newborn nursery) to public spaces;
- Levels of enclosure and safe exit from workspaces;
- Highly hazardous materials (e.g., biological, chemical, radioactive);
- Technology separation and independence; and
- Threats to specific areas, such as pharmacies, health information management spaces, and emergency departments.

These latent conditions can, in part, be mitigated by facility design that addresses site optimization, the building envelope, building layout, unit layout, interior design, and technology. Solutions should take into account the internal forces (culture, organizational policies and procedures) and external forces (regulatory requirements for operation), as well as the workflow and behavior of the facility occupants (staff, patients, families, and visitors).

Mitigating Security Risks With Environmental Design

The majority of material presented in this brief was derived from the International Association for Healthcare Security and Safety (IAHSS) Security Design Guidelines for Healthcare Facilities (IAHSS, 2012).

Site Optimization

Situations requiring emergency planning can be man-made (e.g., terrorism, pandemics), accidental (e.g., fires, hazardous materials), or natural (e.g., earthquakes, hurricanes). To respond to emergencies, coordination between multiple healthcare facilities may be needed, with additional support from public health authorities. Depending on the emergency situation, access to the facility site may need to be controlled. The controlled access points should be identified ahead of time to ensure proper response during emergency situations.
The first level of protection of the healthcare facility is at the perimeter of the site itself. Securing the perimeter with controlled entry points can reduce security-related risks to patients, staff, and families within the facility.

Sufficient lighting is a key component of the surveillance of the site, grounds, and parking lots/structures for the protection of a facility’s perimeter. This can help mitigate risks, as well as facilitate prompt action on any breaches identified.

Places of potential concealment/habitation in the areas surrounding a healthcare building may impede visual surveillance and contribute to a heightened risk of security breaches. Minimizing these areas may help protect a building’s perimeter by enhancing the surveillance of the surrounding site, grounds, and parking structures.

Surface parking lots and multilevel parking structures can be both frightening and dangerous. Control of vehicular access and pedestrian egress, protective barriers, and lighting are effective measures used in practice to create a secure parking facility, both physically and psychologically.

To protect the building at its perimeter, staff members (e.g., those located in a parking attendant booth or security office) need adequate direct visual surveillance of the site, grounds, and parking structures. Direct lines of sight should be provided whenever possible to offer natural surveillance (i.e., non-technological means of observation). It may be difficult for security staff to monitor dead-end parking areas and areas of concealment due to the lack of direct sight lines.

**Building Envelope and Structure**

A second layer of protection should be at the building perimeter, taking into account doors, windows, and other openings, such as those for utility infrastructure, roof hatches, or skylights. Highly security-sensitive areas, such as pharmacies or areas containing protected healthcare information, are at a higher risk for burglary and other security breaches. To protect these security-sensitive areas from unauthorized access, their perimeters should be strengthened through penetration-resistant measures.
Protective elements may also include access-control hardware, intrusion detection, video surveillance, protective glazing materials, or personnel for control and screening at access points. Different facilities may adopt different strategies and levels of technology to secure the building perimeter, but the fundamental goal is to limit and control different access points to allow a more concentrated and effective use of protective measures.

**Building Layout**

The potential for direct visual monitoring of high-traffic areas (e.g., public entrances, waiting areas, information desks) can also help to mitigate security risks, as well as enable prompt action on any breaches identified.

In addition to securing the perimeter, a key strategy for the prevention of unauthorized visitor access to security-sensitive areas is the segregation of authorized and unauthorized visitors (the third layer of protection). The physical segregation (i.e., separated adjacencies, secure doors) may help to prevent unauthorized visitors from accessing security-sensitive areas, such as emergency departments, intensive care units, newborn nurseries, pediatric units, and behavioral health areas.

**Unit Layout**

Public areas often have the fewest restrictions to access, while access-restricted areas are only open to authorized individuals. Separating general public areas, waiting areas, and patient and visitor paths from access-restricted areas can help to contain and manage the risk of unauthorized entrance into the restricted areas. This is a fourth layer of protection that influences both building and unit layouts.

Staff can be vulnerable to attacks or assaults from patients (or even from other staff). To protect the staff, workstations need to be designed after assessing the...
area-specific risk and vulnerability. The potential risk of physical violence to staff may be relatively higher in ED waiting areas or behavioral health units (Blando et al., 2012). Protective measures, such as the degree of enclosure for workstations, may help deter potential violence or unwanted access. For example, staff workstations should have direct access to an exit (i.e., a safe drop-back zone) and duress alarms. This may help protect staff in case of attacks or assaults. (Also refer to the module on Injury of Behavioral Health.)

As with the design of the facility perimeter, direct lines of sight inside a unit can help to mitigate security risks, as well as enable prompt action on any breaches identified. This is especially true in areas associated with aggressive and/or disruptive patients (e.g., emergency departments, behavioral health). The ability to electronically monitor areas associated with aggressive and disruptive patients can also help mitigate security risks and enable prompt action on any breaches identified. These patients may need to be monitored by clinical staff, as well as by security. At the same time, it is important to ensure that patient privacy is protected, since electronic surveillance mechanisms are often invisible to patients.

Highly hazardous materials, including (but not limited to) biological, chemical, and radioactive materials, require the implementation of specific security measures. To prevent harm, it is essential to clearly identify all areas containing hazardous materials, as well as areas of collection and storage. Solutions should be in keeping with the nature of the material and associated regulations.

**HVAC (Heating, Ventilating, and Air Conditioning)**

Chemical and biological hazards are a key concern for the facility infrastructure and can compromise mechanical and HVAC systems. Protecting the HVAC systems from such hazards protects occupants of the facility as well.

**Interior Design and Finishes**

Surveillance systems are often compromised due to wayfinding signage or other obstructions that are put into place without consideration for how direct visual surveillance or electronic surveillance systems may be affected. For example, signs may block the view of CCTV (closed-circuit television) cameras or impede the line of sight from a staffed area to a security-sensitive area.
A healthcare organization is an important member of the community, and each facility may play a role in emergency preparedness. Direct radio communication is important in responding to emergencies and situations of immediate need. In addition, emergencies require facilitated coordination between multiple healthcare facilities, teams, and law enforcement or other agencies. Emergency communication systems should not rely on the building infrastructure (such as power systems), which may be compromised in emergency situations.

Emergencies can result from man-made events (e.g., terrorism, pandemics), accidents (e.g., fires, hazardous materials), or natural disasters (e.g., earthquakes, hurricanes). Emergency planning must take into account various scenarios. Complete lockdown of the facility and site, including shut-down of access and egress systems, may be needed depending on the situation. Within the individual hospital setting (the site and facility), a challenge for security is the use of multiple electronic systems within the facility itself that do not synchronize or communicate with each other, or are not compatible with the physical environment conditions that provide the structure to support electronic and information systems (Yow, 2012). Relevant design elements include power outlets, cabling, and physical location/placement of systems, which may impact the security of electronic/information systems (Yow, 2012). In a hospital, some high-risk areas are not staffed 24/7. Electrical intrusion detection systems can help to detect security risks, as well as notify security staff to enable prompt action on any breaches identified.

**Pharmacies**

Security risks related to central or satellite inpatient and outpatient pharmacies include threat of burglary, threat to personal safety of staff, and threat to property. Securing the pharmacy area with physical separation between the internal operations and public or unauthorized staff access is one design consideration that needs to be balanced with the pharmacy’s accessibility (without compromising security). Separation also includes preventing access through air ducts, cable or utility infrastructure, windows, doors, and dumbwaiters. Different spaces are required to ensure the security of pharmaceutical supplies and for secure medication dispensing. For the context of this safety risk assessment, dispensing occurs in multiple stages: as part of...
the initial delivery, receipt, breakdown, and storage (including narcotic vaults); when medications are distributed from a central location to other areas of the hospital (e.g., carts, dispensing devices, satellite pharmacies, procedure areas, ED); and when medication is delivered to the patient (both inpatients and outpatients).

Security of pharmaceutical supplies can directly impact the security of staff and property and indirectly impact patient safety. Potential routes for accessing pharmaceutical supplies should be blocked to prevent unauthorized access. Providing secured storage may help to prevent unauthorized access to certain hazardous materials and controlled drugs, as well as ensure the security of pharmaceutical supplies.

In addition to the benefits offered to protect staff and supplies, research suggests that a physically separate, uninterrupted area for medication preparation and dispensing activities can aid in reducing medication errors. (Refer to the module for medication safety for additional information.)

Health Information Management Areas

Security of medical records relates to patient rights to information and the safeguarding of patient medical information. It is also at the core of clinical operations at the hospital. One effective method of preventing breaches of access to medical records is physically separating medical records from treatment and public areas, as well as providing lockable storage spaces for medical records.

Emergency Departments (EDs)

EDs are vulnerable to internal as well as external threats that need to be addressed together. ED incidents, including incidences of violence and aggression, are typically recorded by healthcare organizations and can be used for benchmarking and assessing risk. There is a growing body of research around reducing violence in EDs, and it is within the purview of security to mitigate and contain security risks. As with other security-sensitive areas, physically controlling access is a primary consideration. Increased visual surveillance can also help deter and detect attempts at unauthorized entry and other security breaches, and improve response in the case of a security breach.
Disruptive or aggressive patients should be properly monitored and controlled to protect staff and other patients from potential physical and psychological threats, and to improve response in the case of a security breach. Communication systems (e.g., panic buttons) in easy-to-access locations would facilitate the coordination between security, clinicians, and other staff, and accelerate reaction time in case of emergency situations.

Conclusion

Security is a dynamic condition that includes a combination of physical controls and psychological deterrents (York & MacAlister, 2015). The built environment, as one component that influences behavior, is an important part of an overall strategy to reduce vulnerability and mitigate risk to safeguard the physical property and ensure relative safety for facility occupants. Layers of protection should be considered as part of a comprehensive plan that takes into account internal and external forces.

Acknowledgements

The literature review content for the SRA was supported by The Center’s research team (Anjali Joseph, PhD, EDAC; Ellen Taylor, AIA, MBA, EDAC; Xiaobo Quan, PhD, EDAC; and Upali Nanda, PhD, EDAC) and the expert workgroups for each topic area.

References


