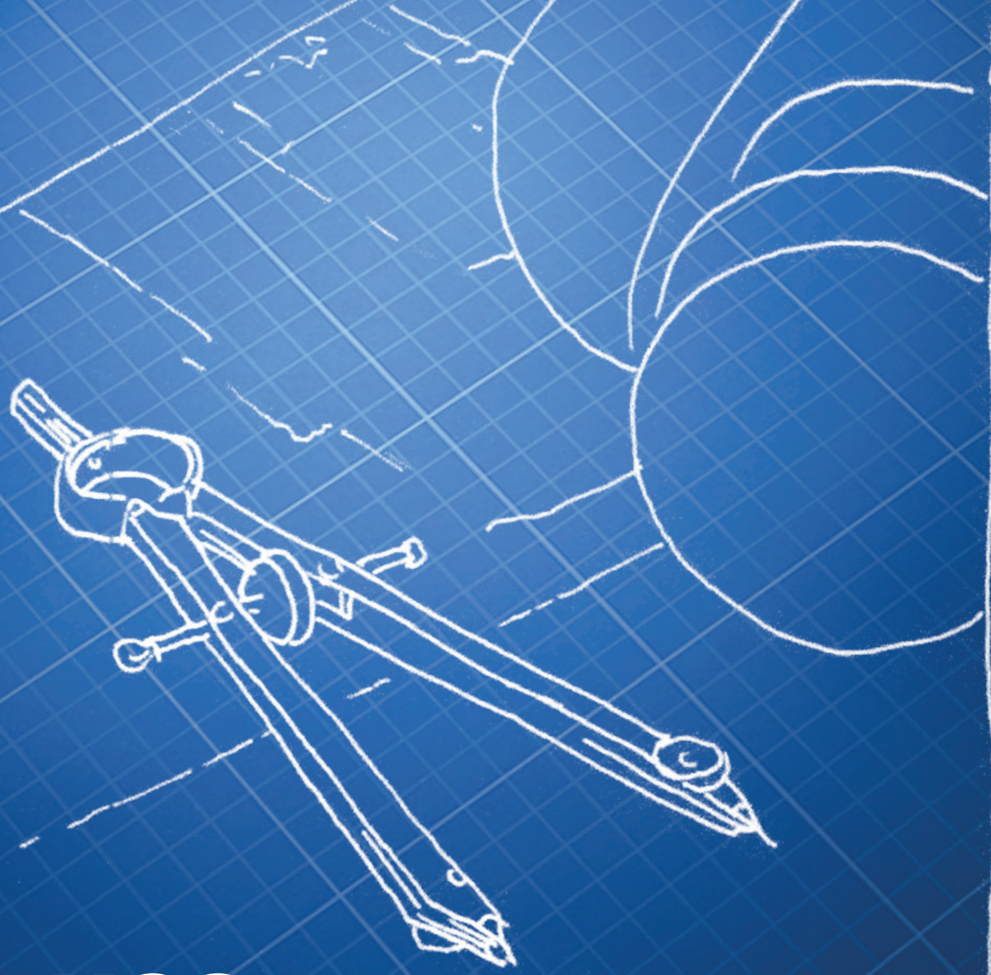
IAHSS

International Association for Healthcare Security & Safety

Security Design Guidelines for Healthcare Facilities



IHSS FOUNDATION

INTERNATIONAL HEALTHCARE SECURITY & SAFETY FOUNDATION

Preface

The 2012 edition of the Security Design Guidelines for Healthcare Facilities was developed by the IAHSS Guidelines Council and funded by the International Healthcare Security & Safety Foundation. These two groups approved and supported the development of a Healthcare Facility Security Design Task Force composed of experts with experience in various aspects of design and development of healthcare facility security programs. The Task Force membership included persons with extensive expertise in design, healthcare security management, physical security, Crime Prevention Through Environmental Design, regulatory agencies, emergency management, healthcare physical plant management and included international representation to ensure the Design Guidelines will also be applicable outside the US.

The first Task Force meeting was in November 2010 and after a thirteen month process, their final work was approved for publication by the Foundation and Association Boards in December of 2011. The Task Force met by phone conference twice per month and held a face to face meeting in early 2011. The vetting process for guideline development included initial development of a guideline topic by a Task Force member, extensive review and discussion by the Task Force, an individual survey of each guideline by the IAHSS membership and interested nonmembers, detailed review by the Guidelines Council, and approval by the IAHSS Board of Directors. After each review comments and suggestions were evaluated and the guideline was revised as appropriate. Ultimately each guideline was approved by consensus of the Guidelines Task Force and Guidelines Council with final approval by the IAHSS Board.

In comparing the IAHSS Basic Industry Guidelines with the Healthcare Facility Design Guidelines readers should be aware that the Basic Industry Guidelines are more operationally focused and less prescriptive. By their nature, the Design Guidelines are more prescriptive and developed to assist security leaders, design professionals and planning staff to build security into each new construction and renovation project. By reasonably addressing security risks up front and early on during design, organizations can cost effectively address the safety and security of new or renovated space. These steps will help reduce the potential for security features either not being designed into new space or added on as an afterthought, or becoming "value engineered" out as projects face limited budget dollars. The intent of integrating these guidelines early in the design process is to emphasize the importance, incorporate the work into other aspects of the project and ultimately to avoid expensive change orders, retrofits or other liabilities incurred by the omission of appropriate planning for a safe and secure environment.

It is our hope that healthcare security and design professionals make use of these design guidelines for every renovation or new construction project. Healthcare Facilities may also choose to develop organizational standards for design based on these standards. We also recommend that the security professional at each healthcare facility use these guidelines as a basis for discussion with their HCFs design staff and customer base. For example, the Design Guideline covering the Emergency Department can be used as a stand-alone guideline and should be forwarded to the department head or manager responsible for that area as a basis for discussion for any future renovation or creation of new space. As these guidelines go to press the Guidelines Council is actively working with other professional groups to help integrate these important concepts with other existing professional design guidelines and standards. Persons with suggestions for improving the Design Guidelines may do so by contacting any member of the IAHSS Guidelines Council.

Acknowledgments

Development of this document took a tremendous effort by the Design Task Force. These individuals dedicated weekends, evenings and their employers allowed them time away from their "day jobs" to facilitate this project. These volunteers received no remuneration for the hours donated to developing this new international guideline.

Although the entire Healthcare Facilities Security Design Guidelines Task Force dedicated a great deal of time and effort, there were three members that took a lead role in developing these guidelines. These three took lead roles in writing and editing the majority of the guidelines. They exceeded all expectations and are deserving of special recognition. My gratitude and very special thanks go out to:

Don MacAlister, Vice President, Paladin Security. In addition to writing several key guidelines, Don organized and developed a completion strategy that kept us on pace with this very demanding work schedule.

Kevin M. Tuohey, Executive Director - Research Compliance, Boston University and Boston Medical Center. Kevin also wrote many of the first drafts. In addition, he worked closely with our editor, Katherine Calver Hawkins, who also works for Boston University. The Office of Research Compliance allowed Katherine, who serves as the Editor for the Research at Boston University publication, to edit this document at no cost to the project and we thank Boston University for this service.

Tony York, Senior Vice President, HSS. Tony is chair of the IAHSS Guidelines Council and worked closely with the IAHSS Board and the IHSSFoundation Board to successfully obtain funding. In addition to writing many first drafts he developed the process for revision and approval of these design guidelines and worked with the Guidelines Council and IAHSS Board to gain acceptance and support for Healthcare Security Design Guidelines.

Tom Smith, CHPA, CPP

Thomas A Smith

Chairman, IAHSS Healthcare Security Design GuidelinesTask Force

Taskforce Members

Chairperson
Thomas A. Smith, CHPA, CPP
Director Police & Transportation
University of NC Hospitals
Chapel Hill, NC

Members
Patrick V. Fiel, Sr.
Public Safety Advisor
ADT Security Services
Wallace, NC

Henry Kosarzycki, A.I.A.
A special thanks to Henry for the graphic design
Architect, Health Care Surveyor
State of Wisconsin Dept. of Health Services
Wisconsin

Donald S. MacAlister, CHPA
Vice President
Paladin Security
Burnaby, BC, Canada

John Reginaldi
Regional Administrator
National Capital Region
Maryland Emergency Management Agency
Reiserstown, MD

Kevin Tuohey, CHPA
Executive Director Research Compliance
Boston University & Medical Center
Boston, MA

Tony York, CHPA, CPP
Senior Vice President
HSS
Denver, CO

Sandy Zirulnik
Presient
SafirRosetti
Oakland, CA

Table of Contents

Glossary of Terms

Access Control: The control of persons, vehicles, and materials through the implementation of security measures for a protected area or areas.

All-Hazards Approach: An approach that emphasizes preparedness for any and all types of hazards and not just for a specific type of hazard. Audit Trail: an examination of records, procedures and practices for the purpose of identifying and correcting unwanted conditions.

Biosafety Level-3 (BSL-3): This level is applicable to clinical, diagnostic, teaching, research, or production facilities in which work is done with indigenous or exotic agents which may cause serious or potentially lethal disease after inhalation It includes various bacteria, parasites and viruses that can cause severe to fatal disease in humans but for which treatments exist.

Buffer Zone: Is known in geography as a zonal area that has the purpose to keep two or more other areas distant from each other and is applied in security design as an area of separation that can be created to help prevent violence and protect an environment.

Closed Circuit Television (CCTV): A video system in which an analog or digital signal travels from a camera to video monitoring stations at a designated location.

Controlled Access Area or Controlled Area: A room, office, building, or facility area which is clearly demarcated of which, access is monitored, limited, and controlled.

Crime Prevention Through Environmental Design (CPTED): For HCFs – emphasizes the proper design and effective use of a designed and built environment to reduce crime and enhance the quality of life. Incorporating CPTED can significantly reduce real or perceived fear and risk of crime as well as the considerable costs associated with adding security equipment and personnel after an incident has occurred or in response to changing standards.

Duress Alarm: A device that enables a person placed under duress to call for help without arousing suspicion.

Dutch Door: An exterior door divided in two horizontally; either half can be closed or open independently.

Electronic Infant Monitoring System: An infant protection system is an electronic security system designed to enhance the safety of infants in obstetric and pediatric departments. Such systems may include a small, tamper-proof tag to be placed on the infant immediately after birth. Should an infant be carried toward an exit door, the system will automatically set off an alarm, activate magnetic door locks and hold selected elevators.

Emergency Operations Center (EOC): Is the physical location where an organization comes together during an emergency to coordinate response and recovery actions and resources. These centers may alternatively be called command centers, situation rooms, war rooms, crisis management centers, or other similar terms. Regardless of the term, this is where the coordination of information and resources takes place. Hospital administrators and other personnel serving in these roles ensure that adequate material and human resources are available to meet the needs of the disaster.

Fire Suppression Systems: Are used in conjunction with smoke detectors and fire alarm systems to improve and increase public safety.The system can operate without human intervention. To do so it must possess a means of detection, actuation and delivery.

Hazard Vulnerability Analysis (HVA): Healthcare Facilities may be required to conduct and annually review their Hazard Vulnerability Analysis (HVA). The HVA provides a systematic approach to recognizing hazards that may affect demand for services or the HCFs ability to provide those services. An HVA may be included in a comprehensive risk assessment.

Healthcare Facility (HCF): Any facility or organization involved in providing healthcare service or treatment simultaneously to four or more patients: who may be primarily incapable of self-preservation due to physical or mental limitation; or who are undergoing treatment or testing which may temporarily render a patient incapable of taking effective action under emergency conditions without assistance from others.

Highly Hazardous Materials: May include, without being limited to biological, chemical or radioactive materials which have the potential to cause immediate and permanent harm at certain exposure levels.

Integrated System: Is an approach that integrates some or all of an organization's systems enabling an organization to review data comprehensively and work more effectively as a single unit with unified objectives.

Intrusion Detection System (IDS): A system combining mechanical or electrical components to perform the functions of sensing, controlling, and announcing unauthorized entry into areas covered by the system. The IDS is intended to sound alarms or alert response personnel of an actual or attempted intrusion into an area.

Magnetometer or Metal Detector: A walk-through portal or hand-held device designed to detect changes in magnetic fields used to identify hidden metal objects/weapons.

Mantrap: A double-door booth or chamber that allows a person to enter at one end, undergo an access identification routine inside the booth, and if the routine is satisfied, the lock on the booth door at other end is released. This approach often compliments the buffer zone approach defined above.

May/Could: Freedom or liberty to follow a suggested or reasonable alternative.

Mitigation: Actions taken to reduce the exposure to and impact of a hazard.Motion Detection: Detection of an intruder by making use of the change in location or orientation in a protected area as the intruder moves around. In video motion detection, this means changes in key parameters of a view scene from a recorded reference image of that scene.

Must/Shall/Will: An imperative need or duty that is essential, indispensable, or mandatory.

Observation / Seclusion Room: This is a room within the emergency department or mental health medical treatment area used to administer care to the combative, uncooperative or 'at-risk' patient.

Physical Security: That part of security concerned with physical measures designed to safeguard people, to prevent unauthorized access to equipment, facilities, material, and documents, and to safeguard against damage and loss.

Protected Area: An area continuously protected by physical security safeguards and access controls.

Protective Glazing Material: Is used to counter many threats to buildings and occupants including bomb (blast) attacks, ballistic attack, burglary or robbery incidents, forced entry, detention containment, and natural disasters such as seismic occurrences, hurricanes and tornados. The proper choice of security glazing is dependent on understanding the desired level of protection.

Protected Health information (PHI): Is any information about health status, provision of health care, or payment for health care that can be linked to a specific individual.

Radio Frequency Identification (RFID): The electromagnetic or electrostatic coupling in the RF portion of the electromagnetic spectrum used to transmit signals. An RFID system consists of an antenna and a transceiver, which reads the RF and transfers the information to a processing device, and a transponder, or tag, which is an integrated circuit containing the RF circuitry and information to be transmitted; an emerging technology that enables companies to better track assets, tools and inventory.

Restricted Area: A controlled room, office, building, or facility area to which access is strictly and tightly controlled. Admittance to this area is limited to personnel assigned to the area and persons who have been specifically authorized access to the area.

Risk: the potential for a loss of or damage to an asset.

Risk Assessment: The overall process of risk identification, risk analysis, risk evaluation and determination of the amount of risk that is acceptable. Note: Risk assessment involves the process of identifying internal and external threats and vulnerabilities, identifying the probability and impact of an event arising from such threats or vulnerabilities, defining critical functions necessary to continue the organization's operations, defining the controls in place necessary to reduce exposure, and evaluating the cost of such controls.

Safe Room: A designated room within the emergency department medical treatment area that can be locked from the inside, as a place for staff, patients, and even visitors to "hide" due to an immediate threat of danger.

Screening: Examining persons and their possessions for contraband such as weapons, explosives, and CBR agents using magnetometer, x-ray, search, or other device.

Security Risk: The potential that a given threat will exploit vulnerabilities to cause loss or damage to an asset.

Security Risk Assessment: The process of identifying threats which could affect personnel, assets or operations, and prioritizing those risks and identifying mitigations strategies and measures. A thorough physical examination of a facility and its systems and procedures, conducted to assess the current level of security, locate deficiencies, and gauge the degree of protection needed. . A Security Risk Assessment may be included in a comprehensive risk assessment.

Security Sensitive Area: A location whose function or activity presents an environment in which there is a significant potential for injury, abduction, or security loss that would most likely severely impact the ability of the organization rendering a high quality of patient care.

Select Agent Laboratories: Are usually regulated and designed to provide commensurate levels of protection to workers given the biological materials that are worked with in such labs. See Biosfaety Level 3 lab definition above

Should: The recommended need and/or duty.

Smart Safes: Are stand-alone electronic safes capable of reading and validating currency. Smart Safes help reduce the risk of fraud and theft.

Terrorism: An action that is intended to cause death or serious bodily harm to civilians or noncombatants, when the purpose of such an act, by its nature or context, is to intimidate a population or to compel a government or an international organization to do or to abstain from doing any act.

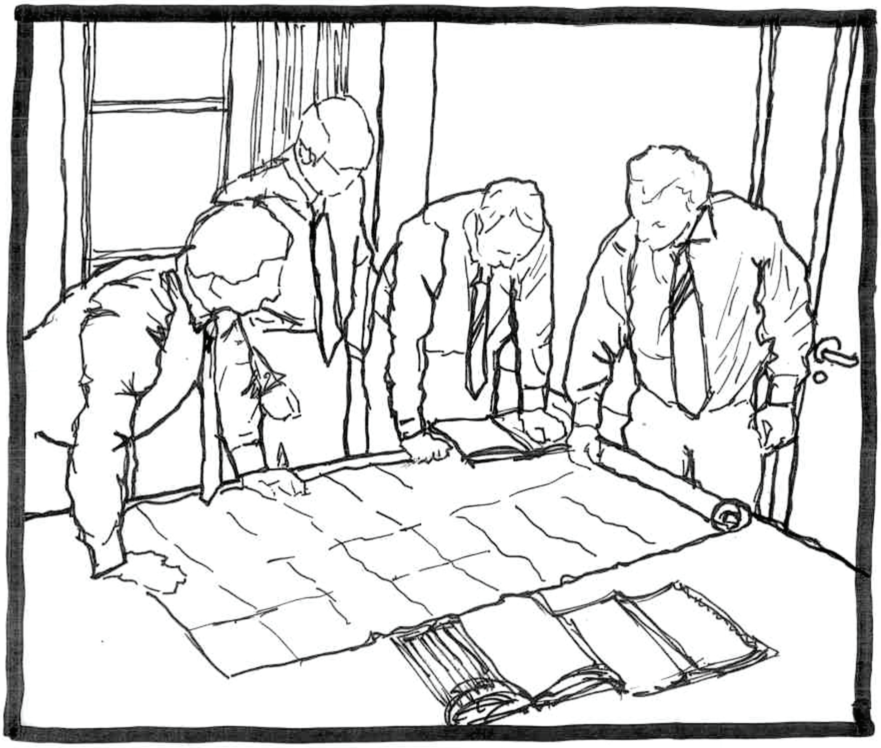
Threat: An indication of impending danger or the type of harm likely to be directed at a facility. The assessment of threat may be included in a comprehensive risk assessment.

Video Intercom System: A solution that allows you to see and talk with individual(s) before admitting them into the facility. By determining a visitor's identity before unlocking the door, you can avoid face-to-face confrontation with a possible dangerous individual.

Video Surveillance: A TV system in which signals are not publicly distributed but are monitored for security and other purpose's; also commonly referred to as CCTV.

Vulnerability: Susceptibility to physical injury or threat.

Vulnerability Assessment: Is a systematic approach used to assess a hospital's security posture, analyze the effectiveness of the existing security program, and identify security weaknesses. . A vulnerability assessment may be included in a comprehensive risk assessment.



General Guideline

STATEMENT: Acts of violence, the potential for crime and terrorism, and the response to and mitigation of emergency incidents are significant concerns for all Healthcare Facilities (HCFs). A consideration of these concerns in the design of new or renovated HCFs presents an opportunity to implement and integrate security design elements that address the delivery of patient care services in a reasonably safe and secure environment, and allows for the cost-effective integration of security applications in architectural, engineering, and environmental design.

INTENT:

a. The IAHSS Security Design Guidelines are intended to provide guidance to healthcare security practitioners, architects, and building owner representatives involved in the design process in order to ensure that these best practices are considered and integrated, where possible, into each new and renovated HCF space.

b. This General Guideline establishes a background and framework for subsequent guidelines covering specific areas of vulnerability and should be utilized as a frame of reference and underpinning for incorporating appropriate security features into the design of all new construction and renovation projects. These guidelines include reference materials that provide further detailed subject matter elaboration.

c. The initial planning and conceptual design phase of all newly constructed or renovated HCFs should include a security risk assessment conducted by a qualified security professional.

d. The size, complexity, and scope of services provided within an HCF can vary significantly. Security design considerations should be risk appropriate for the environment and function, while maintaining design consistency across the HCF. Design considerations should support patient care, provide a positive employee and consumer experience, proactively mitigate risk, and address real and perceived security concerns.

e. The development or continuation of institutional design standards related to the protection of vulnerable patient populations, the securing of sensitive areas, the application of security and safety systems—as well as the infrastructure required to support these needs—are issues best addressed early in the design process to be most cost-effective.

f. The design of HCFs should include consultation with the organizational security representative to identify, design, and provide protective measures. The project design team should prepare and submit plans to the project security representative for review and approval, including a comprehensive security plan that indicates a layered approach. This plan will include zones, control points, circulation routes, and physical security technology locations, and should be reviewed by the security representative prior to submittal to the planning, regulatory, and approval authorities. Integrating these design considerations into the development of submittal documents and through the commissioning process will help avoid costly security and safety retrofits.

g. The integration of these guidelines should be in collaboration with the entire design team. Design considerations should coordinate the security plan, the building Life Safety plan, and the regulations that have jurisdiction in the local environment. This type of coordination will ensure egress paths do not access areas of lower security through areas of higher security.

h. Security requirements for construction, commissioning, and move-in will vary according to the complexity and scope of services provided. A security project plan should be developed that is risk appropriate for the environment and function and should include:
    1. The impact of demolition and phasing of existing site functions and protection efforts.
    2. The need for temporary security barriers such as fencing and security systems, including intrusion and video surveillance.
    3. The installation of security systems should be scheduled for completion to allow for protection of the facility and equipment during early move-in activities.

i. An HCF's surroundings may include open space, parking facilities, and private ways, and may border other businesses, residential properties, major transportation routes, or other areas. The design of HCFs related to site planning is addressed within the Parking and External Campus Environment Design Guideline.

j. HCFs provide care to patients in both inpatient and outpatient areas and may include non-patient care areas such as academic and research space. These areas may present specific risks or security concerns and the design of HCFs related to these types of areas are addressed within the Buildings and the Internal Environment Design Guideline. These areas, which are addressed in specific design guidelines, include:
    1. Inpatient Facilities.
    2. Emergency Department.
    3. Mental Health Areas.
    4. Pharmacies.
    5. Cashier and Cash Collection Areas.
    6. Infant and Pediatric Facilities.
    7. Protected Health Information Areas.
    8. Utility, Mechanical, and Infrastructure Areas.
    9. Biological, Chemical, and Radiation Areas.

k. HCFs frequently provide both scheduled and emergency services, serve as part of local emergency response networks, and are frequently expected to be functional, safe, and secure for patients, visitors, and staff while remaining prepared for natural and man-made emergencies 24/7. The design of HCFs related to these types of issues is addressed within the Emergency Management Design Guideline.

l. The development of the Security Design Guidelines for Healthcare Facilities reflects the principles of Crime Prevention Through Environmental Design (CPTED). These principles, when applied early, can be integrated into any HCF design providing layers of protection for patients, visitors, and staff.

m. CPTED defines territories and how they are controlled and managed based on the use of "concentric rings of control and protection." Outermost rings are supported by additional inner rings of protection. Each of these concentric rings will be addressed as layers of protection within these guidelines and are intended to sequentially deter, deny access to, and slow down possible malefactors. In the healthcare environment, CPTED layers may include:

1. *The first layer of protection should be at the perimeter of the property, which limits points of entry. The campus perimeter should be defined by fences, landscape, or other barriers. At certain locations, this may include the building exterior. Campus entry points should be controllable during emergency situations or heightened security levels.*
2. *The second layer of protection should be at the building perimeter and consist of doors, windows, or other openings. Protective elements or components may include access-control hardware, intrusion detection, video surveillance, use of protective glazing materials, or personnel for control and screening at selected entrances during designated times.*
3. *The third layer of protection should be inside the building itself, segregating authorized and unauthorized visitors. Using physical and psychological barriers and hardware, this layer is most frequently applied in areas of higher risk such as emergency treatment areas, intensive care units, mental health areas, pediatric units, newborn nurseries, and recovery rooms.*
4. *The fourth layer of protection should segregate generally accessible public and patient areas and staff-only areas. Using physical barriers and locking hardware, this layer is most frequently applied to areas that restrict all visitors and limit access to HCF staff only in areas such as nursing offices, staff locker rooms, storage and distribution locations, food preparation, sterile corridors, and research laboratories.*
5. *The fifth layer of protection should further restrict staff access to highly sensitive areas. Using physical barriers and locking hardware, this layer is most frequently applied to areas that are limited to vetted and authorized HCF staff. These areas frequently include the pharmacy and narcotic storage spaces, hazardous materials, plant utility and information technology infrastructure, and areas housing personal health information (PHI). Security design considerations for such areas should be addressed in accordance with applicable regulatory oversight, standards, and guidelines.*

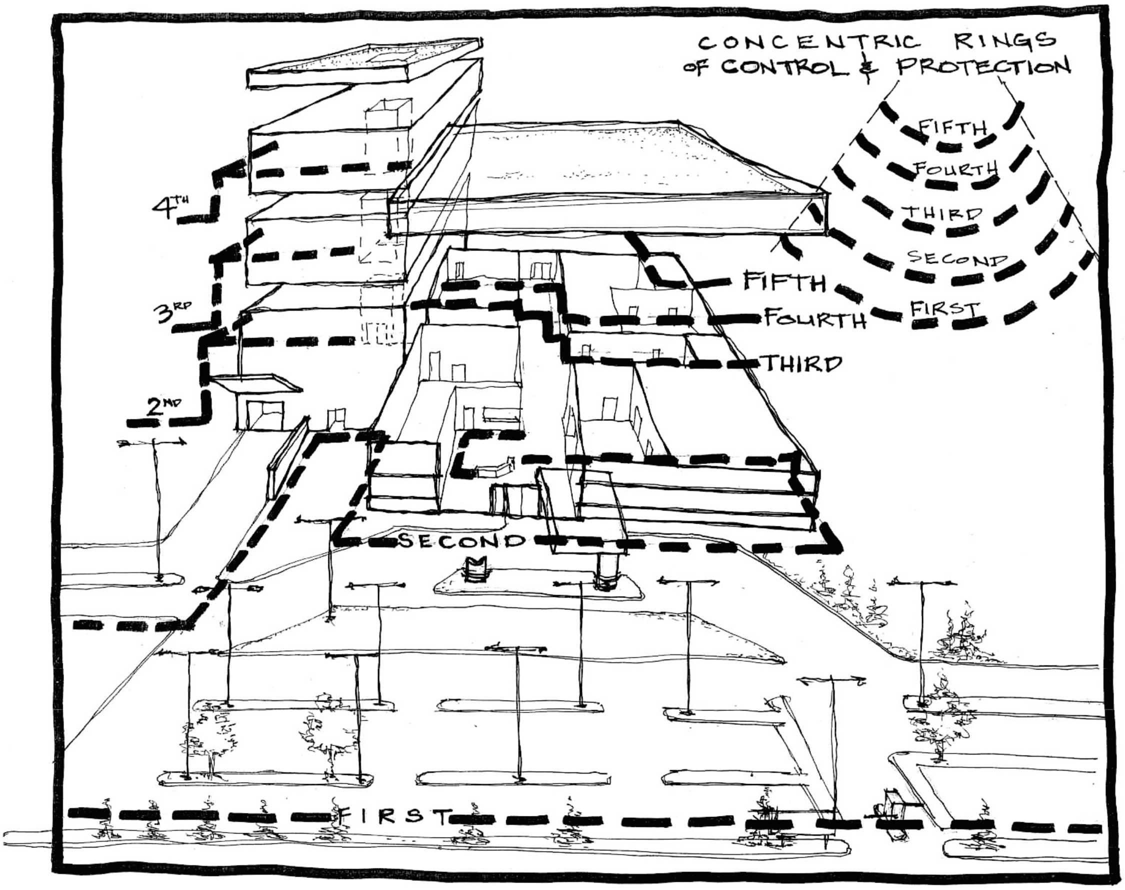
REFERENCES/GENERAL INFORMATION:

Physical Security Design Manual for VA Facilities: Mission Critical Facilities: www.wbdg.org/ccb/VA/VAPHYS/dmphysecmc.pdf

International CPTED Association (ICA): www.cpted.net/

SEE ALSO:

IAHSS Healthcare Security: Basic Industry Guidelines: www.iahss.org/About/Guidelines-Preview.asp


CONCENTRIC RINGS
OF CONTROL & PROTECTION
FIFTH
FOURTH
THIRD
SECOND
FIRST
4TH
3RD
2ND
FIFTH
FOURTH
THIRD
SECOND
FIRST

01. Parking and the External Campus Environment

STATEMENT: The security of parking facilities and the external campus environment is a significant concern for Healthcare Facilities (HCFs) and for users of those facilities. The proper design and effective management of the external campus environment can minimize violent and property crime, promote efficient resource management, and provide a welcoming environment.

INTENT:

a. This guideline complements the Security Design Guidelines for Healthcare Facilities, General Guideline.

b. The initial planning and conceptual design phase of the external campus and new or renovated parking facilities should include a security risk assessment conducted by a qualified healthcare security professional.

c. The project design team should prepare and submit plans to the project security representative for review and approval, including a comprehensive exterior site security plan that indicates a layered approach, including zones, control points, circulation routes, landscaping, and illumination.

d. Landscape plans should be designed to enhance lighting, eliminate places of potential concealment or habitation, and address obstructions to surveillance or lighting systems.

e. Physical protective barriers should be placed at building entrances and walkways to minimize the likelihood of injury or damage by vehicles to pedestrians, equipment, and structures.

f. The external environment should be addressed from the outside inwards and the first point of control should be at the perimeter of the property limiting points of entry. Access control and perimeter security should be considered in the initial design stage.

1. Physical protective barriers should be designed to help restrict or channel access.
2. Natural barriers, landscaping, or security fencing should be considered to discourage persons from entering the campus unobserved on foot while maintaining openness and allowing for natural surveillance.
3. Transit, taxi, and pickup/drop off stops should be identified and situated to maintain perimeter control and prevent unobserved pedestrian access.

h. Lighting should be installed. To be effective, protective lighting should:

1. Act as a deterrent and allow for effective recognition of persons and activities.
2. Be constructed with a shatter-resistant lens, designed to withstand environmental degradation of light output, and provide protection from vandalism.
3. Have properly fitted enclosures that prevent insects and debris from accumulating within the fixture.
4. Be selected and positioned to avoid glare and blind spots.
5. Be designed to provide adequate redundancy of lighting in the event of an occasional loss of service.
6. Be automatically supported by standby power.

7. Be installed to prevent light pollution or light trespass into the surrounding community.
8. Be integrated with the video surveillance system design to ensure adequate coverage.
9. Include environmentally sustainable features that do not hinder the effectiveness of protective lighting.

h. Way-finding signage should be used to orient and guide patients and visitors to their desired location. To be effective, signage should:
   1. Provide clear and consistent messaging.
   2. Use color coding or memory aids to help individuals locate their vehicle.
   3. Be used to enhance security awareness in parking areas while serving as psychological deterrent to criminal and other negative behavior.
   4. Not obstruct natural sight lines.

i. The HCF should provide dedicated patient and visitor parking where possible. Additional parking considerations should be provided for emergency care patients, on-call clinicians, public safety, valet parking, and those working during non-traditional hours.

j. Security considerations for parking facilities, including surface lots, should include the following safeguards:
   1. Concentrating pedestrian egress paths to dedicated entrances and exits.
   2. Limiting the number of vehicular entrances and exits.
   3. Locating attendant booths, parking offices, and security stations where attendants can directly monitor parking activity (if appropriate).
   4. Installing emergency communication devices along pedestrian walkways.
   5. Installing video surveillance to obtain images of all:
      a) Vehicular and pedestrian entrances and exits.
      b) Areas of higher traffic activity.
      c) Emergency communication devices.
      d) Attendant booths.
   6. Absence of public restrooms in unstaffed areas.

k. Security considerations specific to parking structures should include the following safeguards:
   1. Maximizing the visibility into and within the parking structure.
   2. Enhancing natural surveillance and line of sight.
   3. Using white concrete stain to increase general brightness and enhance illumination. Painting is discouraged as it can require increased maintenance.

Anti-graffiti coatings should be considered to enable quick and easy cleaning.

4. Installing two-way emergency communication devices on each level of the structure and in all elevators.
5. Locating elevators and stairs on the perimeter with material that allows natural surveillance from exterior public areas.
6. Concentrating pedestrian paths to dedicated entry/exit portals. Emergency exits should be designed for egress only.
7. Features that prevent and deter entry by unauthorized persons, including, but not limited to, fencing, grates, metal grills, landscaping, or other protective measures.
8. Closing off potential hiding places below stairs.
9. Avoiding dead-end parking areas and areas of concealment.
10. Including in the design the ability to completely shut down vehicular and pedestrian access to the parking facility when closed.

REFERENCES / GENERAL INFORMATION:

Illuminating Engineering Society of North America, Lighting for Emergency, Safety and Security, 2011.

National Institute of Justice, Crime Prevention Through Environmental Design in Parking Facilities, April 1996: www.ncjrs.gov/pdffiles/cptedpkg.pdf

SEE ALSO:

IAHSS Basic Industry Guideline 09.10.01 – Parking (General).

02. Buildings and the Internal Environment

STATEMENT: The physical design of buildings and integration of electronic security systems within the internal built environment are important components of the Healthcare Facility (HCF) protection plan and the patient, visitor, and staff experience. Security design considerations must address the particular requirements and services offered by the HCF.

INTENT:

a. This guideline complements the Security Design Guidelines for Healthcare Facilities, General Guideline.

b. The initial planning and conceptual design phase of new or renovated buildings or space should include a security risk assessment conducted by a qualified healthcare security professional.

c. The project design team should prepare and submit plans to the project security representative for review and approval, including a comprehensive security plan that indicates a layered approach, including zones, control points, circulation routes, and required egress paths.

d. The size, complexity, and scope of services provided within an HCF can vary significantly; in all cases, the building design should be composed of defined zones of protection. Typical zones in the healthcare environment may include:

    1. General areas accessible to the public at all times.
    2. General areas restricted to the public during non-visiting hours or periods of lesser activity.
    3. Screened public areas.
    4. Staff and accompanied public areas.
    5. General staff-only areas.
    6. Areas for designated staff with the appropriate clearance.

e. The internal environment should be designed to address horizontal and vertical circulation routes that facilitate operational functions in accordance with security needs and life-safety requirements. Physical separations should be provided between general public areas, waiting areas, and access-restricted areas.

f. The inclusion of a risk assessment in initial design will allow determination of needs related to the access from zones of lesser security to zones of higher security and will help in identifying the appropriate methods of control that may include signage, physical barriers, direct staff supervision, mechanical and electronic access controls, and audible or monitored alarms.

g. The access to all staff-only entry points, circulation points, elevators, and stairwells should be controlled and restricted.

h. The management of access systems should be consistent across the HCF as to the operating procedures and type of systems used. Electronic security systems, if available, should be integrated and standardized. Design considerations for electronic safeguards should include:

    1. Designating the location of duress alarm buttons at strategic locations where

employees work alone, in isolated areas, or other areas of higher risk as identified by the security risk assessment.

2. Using video surveillance to capture and record images in defined security sensitive areas or other areas of higher risk as identified by the security risk assessment. Each camera application should have a defined philosophy of use that is consistent within the area being protected, recognized industry best-practices, and regulatory standards.
3. Selecting and specifying door and window hardware with specific security requirements and functionality. Hardware should be durable and appropriate for the environment.
4. Coordinating door hardware, security electronic systems, electrical, and fire alarm system specifications.
5. Installing security intrusion systems in non-24-hour facilities on all entry portals and in other areas of higher risk as identified by the security risk assessment. The installed system should be designed to allow independent arming of various areas of the building in support of different departmental hours of operation.
6. Developing a coordinated signage approach for way-finding, brand identification, security, and emergency information and, if possible, mass notification.
7. Avoiding, where possible, stand-alone systems for individual buildings or renovation projects.
8. Implementing 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.
9. Future-proofing security systems by providing flexible infrastructure, including wiring pathways and equipment locations.
10. Coordinating with other building technology systems, as appropriate.

i. The determination of where building security systems will be monitored and controlled should address the need for adequate space and environmental conditions in support of electronic equipment. If offsite, provisions should be made for support spaces for electronic equipment within the facility and infrastructure necessary for connectivity to offsite monitoring and control systems.

j. Public and patient care areas in general should have securely fastened electronics, wall hangings, plants, fire extinguishers, or other hard objects.

k. Design considerations for security-sensitive areas are addressed in separate guidelines. Other areas requiring consideration include:

1. Materials management, central supply/store, and sterile processing should include:
   a) Designation as authorized staff-only areas.
   b) Controlled and restricted access in and out of area.

   c) Electronic access control for frequently used staff doors.
   d) Hardened walls, ceiling, and doors to prevent penetration.
   e) Secure storage for items of higher value.
   f) Video surveillance.
   g) Intrusion detection systems for monitoring during non-occupied hours.

2. Shipping and receiving/loading docks should include:
   a) Locations away from patient care areas and critical infrastructure.
   b) Designation as authorized staff-only areas.
   c) Controlled and restricted access in and out of area.
   d) Electronic access control for frequently used staff doors.
   f) Hardened walls, ceiling, and doors to prevent penetration.
   g) Secure storage (e.g., fencing, gates, or locked cages for items of higher value, hazardous materials, or items with personal health information).
   h) Video surveillance to obtain images of all entry and exit points.
   i) Fencing, cargo doors, or other means to secure the external loading dock area from surrounding streets.

3. Mail rooms should include :
   a) Locating mail receiving and sorting rooms away from critical building infrastructure and structural support and mission-critical building functions, if possible at an offsite central receiving facility.
   b) Location on the building perimeter, near or adjacent to the loading dock.
   c) Designation as general staff-only areas.
   d) Controlled and restricted access in and out of area.
   e) Electronic access control for frequently used staff doors.
   f) Secure storage (e.g., lock boxes or other secure means for items with personal health information).
   g) Video surveillance to obtain images of all entry and exit points.

4. Health information management (medical records) should include:
   a) Designation as authorized staff-only areas.
   b) Controlled and restricted access in and out of area.
   c) Electronic access control for frequently used staff doors, maintaining an audit record of room access.
   e) Hardened walls, ceiling, and doors to prevent penetration.
   f) Video surveillance to obtain images of all entry and exit points.

g) Intrusion detection systems for monitoring during non-occupied hours.

5. Human resources, administrative, executive, and business offices should include:

   a) Designation as general staff and accompanied public areas.

   b) Controlled and restricted access in and out of areas after normal business hours or when areas are not occupied.

   c) A reception room or vestibule for areas requiring public interface separate from staff workstations.

   d) Video surveillance to obtain images of all entry and exit points, cash handling, safe locations, and reception areas.

   e) Secure cash storage in areas where cash is collected or stored.

   f) Duress alarms at reception areas and human resource and executive offices.

   g) Intrusion detection systems for monitoring during non-occupied hours.

6. Meeting rooms and conference areas should include:

   a) Designation as general staff and accompanied public areas.

   b) Controlled and restricted access in and out of area after normal business hours or when areas are not occupied.

   c) Appropriate circulation and egress paths.

   d) Secure storage for high-value audio/video equipment, computers, and other office equipment.

7. Call centers, switchboard, or other staffed telephone answering rooms should include:

   a) Designation as authorized staff-only areas.

   b) Controlled and restricted access in and out of areas.

   c) Electronic access control for frequently used staff doors, maintaining an audit record of room access.

   d) Direct communication capability with security, law enforcement, and other public safety agencies.

8. Research facilities, whether stand-alone or integrated with other healthcare operations, should include:

   a) Evaluating the specific threats and risks associated with all research activities (current and future) to include performing a formal risk assessment for animal research facilities and Bio Safety Level (BSL) 3 and 4 laboratories.

b) Designation as authorized staff-only areas.

c) Controlled and restricted access in and out of areas.

e) Electronic access control for frequently used staff doors, maintaining an audit record of access.

f) Hardened walls, ceiling, and doors to prevent penetration.

g) Video surveillance to obtain images of all entry and exit points.

h) Intrusion detection systems for monitoring during non-occupied hours.

9. Childcare centers, whether stand-alone or integrated with other healthcare operations, should include:

a) Designation as authorized staff-only areas.

b) Controlled and restricted access in and out of areas.

c) Electronic access control for frequently used staff doors, maintaining an audit record of facility access.

d) Appropriate circulation and egress paths.

e) Video surveillance to obtain images of all entry and exit points.

f) Intrusion detection systems for monitoring during non-occupied hours.

g) Monitored electronic abduction prevention or wander alert system should be utilized based on the assessed vulnerability of the population served.

10. Urgent care facilities, whether stand-alone or integrated with other healthcare operations or medical office buildings, should include:

a) Clear distinction and control between general public waiting areas and medical treatment areas.

b) Controlled and restricted access in and out of medical treatment areas.

c) Electronic access control for frequently used staff doors, maintaining an audit record of area access.

d) Appropriate circulation and egress paths.

e) Video surveillance to obtain images of all entry and exit points and waiting areas.

g) Intrusion detection systems for monitoring during non-occupied hours.

h) Registration desks positioned to provide staff direct access to an exit portal (safe drop-back zone) and equipped with strategically located duress alarms.

11. Operating rooms, sterile areas, and special procedures areas should include:

a) Designation as authorized staff-only areas.

b) Controlled and restricted access in and out of areas.

c) Electronic access control for frequently used staff doors, maintaining an audit record of access.

d) Video surveillance to obtain images of all entry and exit points.

e) Secure storage or other secure means for storing controlled substances and items of higher value (e.g., surgical instruments).

REFERENCES / GENERAL INFORMATION:

OSHA Guidelines for the Prevention of Workplace Violence in the Healthcare and Social Work Settings: www.osha.gov/Publications/OSHA3148/osha3148.html

OSHA Enforcement Procedures for Investigating or Inspecting Incidents of Workplace Violence CPL 02-01-052: www.osha.gov/OshDoc/Directive_pdf/CPL_02-01-052.pdf

Physical Security Design Manual for VA Facilities: Mission Critical Facilities: www.wbdg.org/ccb/VA/VAPHYS/dmphysecmc.pdf

Whole Building Design Guide summary of design standards for mail rooms: www.wbdg.org/design/mail_center.php

SEE ALSO:

IAHSS Basic Industry Guideline 09.01 Security Sensitive Areas.

02. Buildings and the Internal Environment
01. Inpatient Facilities

STATEMENT: A safe and secure environment contributes to the quality of care rendered by inpatient Healthcare Facilities (HCFs). Security design considerations must address the particular risks associated with the services offered by the inpatient HCF, patient demographics, and other environmental factors.

INTENT:

a. This guideline complements the Security Design Guidelines for Healthcare Facilities, Parking and the External Campus Environment Guideline #01, and Buildings and the Internal Environment Guideline #02.

b. The initial planning and conceptual design phase of new or renovated inpatient space should include a security risk assessment conducted by a qualified healthcare security professional.

c. The project design team—including the project security representative—should develop a comprehensive security plan that indicates a layered approach, including zones, control points, circulation routes, and required egress paths.

d. The physical design of the inpatient HCF should support a visitor reception and screening process during and after normal business hours. Patients and visitors presenting to the HCF on foot and in vehicles should be funneled to entries with staffed reception areas where assistance, general guidance, and a psychological deterrence to wrongdoing can be provided. Ideally, the number of staffed reception areas should be minimized.

e. Designated after-hours access points for visitors should be identified during the design phase. Physical controls or barriers should be provided to clearly distinguish between public areas and waiting areas supported by the entrance and other HCF locations.

f. Access to all staff-only entry points, circulation points, elevators, and stairwells should be controlled and restricted.

g. Elevators available to the public should be located outside of the controlled patient care area. Emergency egress paths should be provided for all elevator lobby locations that are outside of the controlled patient care area. Consider designated staff-only elevators to serve back-of-house areas such as surgery, emergency department, materials management, and central supply. Provide electronic access control or other means to restrict the use of these elevators.

h. Exterior windows located throughout the inpatient HCF should be treated to prevent internal viewing from outside of the facility.

i. Design considerations for reception desk, information desks, and other screening stations should include:

   1. Clear distinction and control between work stations and general public areas.
   2. Protection to prevent unwanted access and be of sufficient height and strength to make it difficult for someone to jump over a barrier or physically assault an employee. The degree of enclosure and protective material used should depend on the assessed vulnerability.
   3. Positioned to provide staff direct access to an exit portal (safe drop-back zone) and equipped with strategically located duress alarms.
   4. Adequate workstation space that can support a visitor pass issuance process and related equipment.

j. Waiting areas should be outfitted with furniture pieces that are attached to each other or secured to the floor or a wall. Small or individual pieces should not be used. Wall hangings, coat hooks, and other hung objects should be positioned at a height so to not present a safety risk to an average-sized person while maintaining clear sight paths.

k. Security officer posts and/or police officer workstations, if applicable, should be located to maximize visibility at public entrances, waiting areas, registration, and information areas.

l. Signage should be provided to assist patients and visitors with way-finding, including appropriate pathways to patient rooms and diagnosis and treatment areas. These patient and visitor paths should be considered "screened public" and should not pass through designated staff-only security zones.

m. Access to special care areas should be limited. Access to all doors, interior elevators, and stairwells into intensive care and other critical care areas should be controlled and restricted to authorized personnel only. Doors leading to each should be equipped with authorized staff-keyed hardware and a clearly marked communication station on the exterior side of the entrance with direct visual observation capability or a video surveillance system to manage the control system.

n. Inpatients are often compromised in mobility and level of consciousness and require additional protection by the facility. Ideally, the HCF should control access to areas hosting general inpatient rooms. Reception and entry to these areas should be provided by staff with direct visual observation capability or a video surveillance system to manage the control system.

o. Security design considerations for inpatient rooms should include secure storage for patient valuables and other items of higher value.

p. On-call staff sleeping rooms and suites should be equipped with appropriate locking hardware on entry doors. Strategically located duress alarms should be considered for staff sleeping rooms.

q. Access to staff lockers and lounges should be controlled at all times and restricted to authorized staff only. Locked storage or other means of control should be provided for clean and soiled staff uniforms.

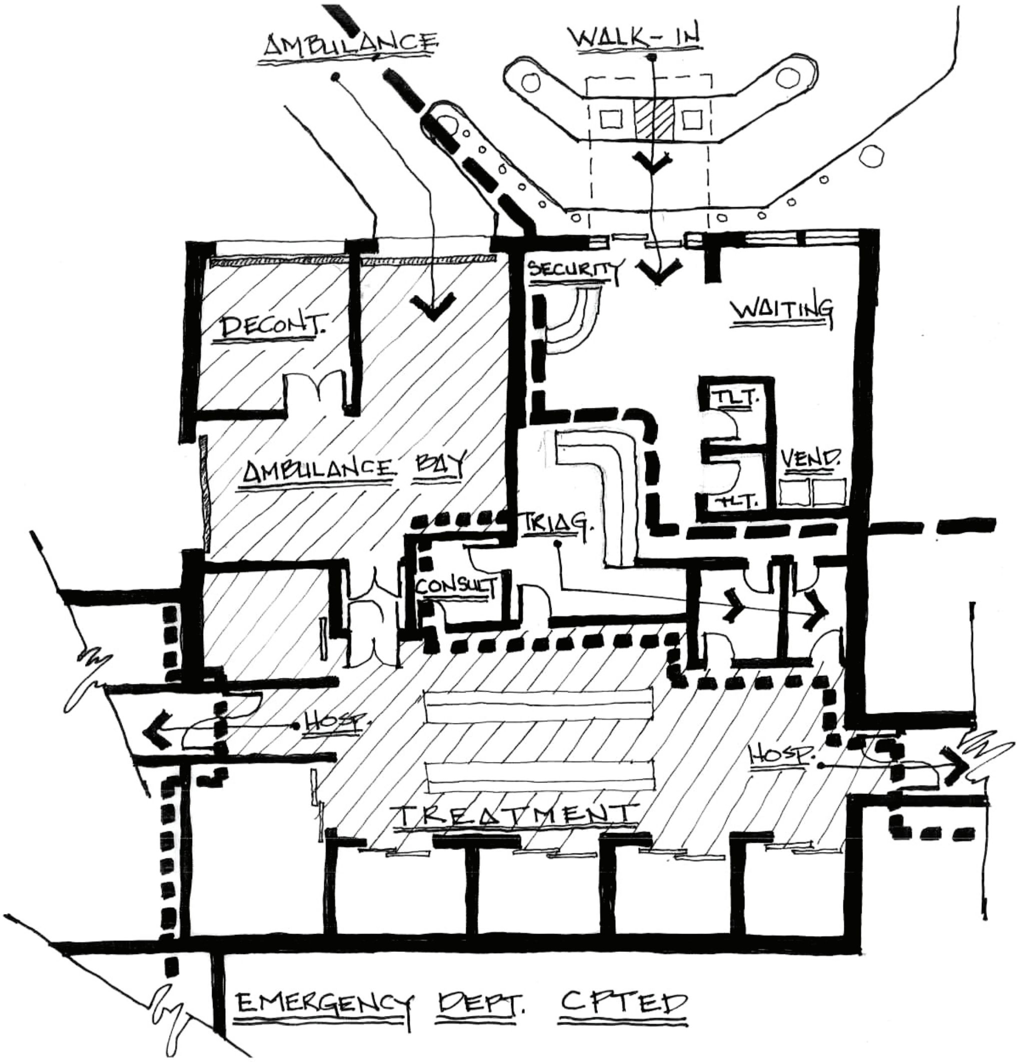
REFERENCES / GENERAL INFORMATION:

Physical Security Design Manual for VA Facilities: Mission Critical Facilities: www.wbdg.org/ccb/VA/VAPHYS/dmphysecmc.pdf

International CPTED Association: www.cpted.net/

SEE ALSO:

IAHSS Basic Industry Guideline 09.01 Security Sensitive Areas.


AMBULANCE
WALK-IN
SECURITY
WAITING
DECONT.
AMBULANCE BAY
TLT.
VEND.
TLT.
TRIAG.
CONSULT
HOSP.
HOSP.
TREATMENT
EMERGENCY DEPT. CPTED

STATEMENT: The physical design of the Emergency Department (ED) should promote an all-hazards approach to the safety and security of those working in, visiting, or seeking emergency services from the Healthcare Facility (HCF).The security layout and design of the ED should be viewed as a secured area that serves as an added layer of protection between the HCF, public areas, and treatment areas.

INTENT:

a. This guideline complements the Security Design Guidelines for Healthcare Facilities, Parking, and the External Campus Environment Guideline #01 and Buildings and the Internal Environment Guideline #02.

b. The initial planning and conceptual design phase of new or renovated ED space should include a security risk assessment conducted by a qualified healthcare security professional.

c. The project design team—including the project security representative—should develop a comprehensive security plan that indicates a layered approach, including zones, control points, circulation routes, and required egress paths.

d. The HCF should include design of adjacent spaces providing access, support, protection, or services related to the support of ED functions.

   1. The HCF should provide dedicated parking for emergency care patients. Signage should provide clear and consistent messaging and easily guide patients and visitors from the dedicated parking area to the ED entrance.
   2. ED entrances should be positioned at an angle from driveways and parking areas to prevent intentional or accidental ramming of doors. Solid physical barriers, curb markings, or other visible psychological deterrent means should separate the entrances from sidewalks and facility drives.
   3. There should be clear distinction between the ambulance and walk-in entrance that is clearly marked and provides a reasonable degree of separation between the two. The line of sight between these entrances should be disrupted using physical or other visual barriers.
   4. Dedicated parking areas, ED entrances, dedicated waiting areas, ambulance bays, and other patient access points should contain adequate lighting, video surveillance, and equipment to facilitate communication with care providers, security staff or other designated personnel.
   5. The type of exterior wall and protective material used should depend on the assessed risk/vulnerability.

e. The HCF should address ED-specific security design needs, including:

   1. All external ED entrances should be equipped with the ability to quickly restrict access into the facility.
   2. The ED walk-in entrance may be equipped with a video monitor displaying live camera images of all persons entering for public viewing and awareness.
   3. The ambulance entrance should be controlled and restricted to authorized ambulance drivers and HCF personnel only. Doors should be visible to a

nursing station and be equipped with a clearly marked communication station on the exterior side of the entrance with direct visual observation capability or a video surveillance system to manage the control system.

4. Metal screening should be utilized based on the assessed vulnerability of the population served (present and future). Design considerations should include queuing of patients and visitors and screening prior to access to the waiting area, or prior to entering the treatment space.
5. Secure storage for weapons, patient valuables, and other items of higher value should be provided within the ED or in close proximity.
6. ED signage should provide clear messages depicting authorized passage points for patients and visitors and HCF staff. Access to the HCF provided from the ED should be controlled to the greatest degree possible.
7. The patient and visitor waiting area space should be compartmentalized with:
    a) One primary access control point.
    b) Washrooms, vending equipment, and telephones.
    c) Visitor comforts to help with time passage (e.g., television, internet access).
    d) Securely fastened wall hangings, plants, fire extinguishers, or other hard objects.
    e) Video surveillance.
8. Furniture used in ED waiting areas should include pieces affixed to each other, the floor, or the wall. Small or singular pieces should not be used. Windows in the ED waiting area and throughout the ED should be covered to prevent internal viewing from the outside. Wall hangings, coat hooks, and other hung objects should be positioned at a height so to not present a safety risk to an average-sized person while maintaining clear sight paths.
9. Security/police officer workstations (if applicable) should be visible from the ED waiting area, registration, and triage areas (if possible).
10. There should be clear distinction between registration/admitting desks and the ED waiting area. Work areas should be protected to prevent unwanted access and be of sufficient height and strength to make it difficult for someone to jump over a barrier or assault an employee. The degree of enclosure and protective material used should depend on the assessed risk/vulnerability. Workstations should be positioned to provide direct access to an exit portal (safe drop-back zone) and equipped with strategically located duress alarms.
11. A family consult room should be located between the waiting and the medical care area with open access from the waiting area and restricted access to the medical care area.
12. There should be clear distinction between triage and the ED waiting area. The

line of sight between triage workstations and the ED walk-in entry should not be disrupted. Triage access should be controlled with two points of entry/exit for staff. Care provider workstation(s) should be positioned to provide direct access to an exit portal (safe drop-back zone) and equipped with strategically located duress alarms.

13. Access to medical treatment areas, including all doors, interior elevators, and stairwells should be controlled and restricted to authorized HCF personnel only. Doors should be equipped with a clearly marked communication device on the exterior side of the entrance with direct visual observation capability or a video surveillance system to manage the control system. Relationships with other departments should be considered when designing the medical treatment area (e.g., radiology).
14. Nursing stations should be of sufficient height and strength to make it difficult for someone to jump over a barrier or assault an employee and include multiple points of entry/exit. Workstations should be equipped with strategically located duress alarms and video surveillance monitors for high-risk patient rooms. Clear sight paths from the nursing station to patient care rooms within responsible care area should be maintained.
15. The patient care area in general should contain securely fastened wall hangings, plants, fire extinguishers, or other hard objects.
16. The standard patient room should position the patient bed in the center of the room providing staff access at a minimum of three sides. In-room televisions should be high-mounted with coat hooks and other hard-affixed objects positioned at a height so to not present a safety risk to an average-sized person. Wall-mounted computer workstations located in the room should allow unimpeded exit and continuous patient view. All cabinetry should be lockable. All patient rooms should allow for unimpeded observation by clinical staff from outside the room.
17. Staff lockers and lounges located within the ED should be controlled at all times and restricted to authorized HCF staff only.
18. A designated safe room may be established within the ED that that can be locked from the inside as a place for staff, patients, and even visitors to retreat in the event of an immediate threat of danger. The safe room should be equipped with a duress button, telephone, reinforced doors with a peep-hole installed, and external lock and key access.
19. Video surveillance should be used to capture and record an image of all persons leaving the medical treatment area.

f. The HCF should include the following guidelines if services are, or will be, provided to high-risk patient populations:

1. High-risk patient/observation rooms that may be used for disruptive or aggressive patients or those at risk of elopement should be designated based on the assessed vulnerability of the patient population served (present and future). Design considerations should include:
   a) Isolating the patient, distancing the patient from department exits, locating the patient in close proximity to dedicated rest rooms, and providing for direct observation of room by clinical staff.
   b) Positioning multiple observation rooms in close proximity.
   c) Incorporating video surveillance with audio capability to remotely monitor patient activity; cameras should be enclosed in tamper-proof housing. Monitoring locations should meet patient privacy and clinical requirements.
   d) Controlling access in and out of room or suite of rooms, if used.
   e) Equipping doors with tamper-proof hardware and observation window with window coverings managed from outside of the room.
   f) Hardening walls, ceiling, and doors to prevent penetration.
   g) Equipping the room with removable objects and protecting medical equipment behind locked cabinetry, gates, impact-resistant laminate, or other hardened material.
   h) Incorporating safety measures that mitigate the potential for a patient to cause harm to themselves or others.
   i) Using protective hardware for wall hangings.
   j) Considering the installation of televisions to assist in occupying patients held over for extended periods of time. These televisions should be mounted behind protective glazing.
   k) Positioning patient restraint storage in close proximity.
2. An appropriate number of forensic (prisoner) patient rooms should be designated based on the assessed vulnerability and relationships the HCF has established with external law enforcement agencies. Design considerations should include:
   a). Controlling and restricting access into the room continuously, and locating one point of access/egress off of the ambulance bay and a second from inside the medical care area.
   b) Incorporating video surveillance with audio capability to monitor all activity; cameras should be enclosed in tamper-proof housing.
   c) Equipping doors with tamper-proof hardware and observation window with window coverings managed from outside of the room.

d) Equipping the room with removable objects and protecting medical equipment behind locked cabinetry, gates, impact-resistant laminate, orother hardened material.

e) Hardening walls, ceiling, and doors to prevent penetration; providing floor tie downs for shackles.

f) Positioning gun lockers in ambulance bay vestibule.

g. Decontamination rooms or other services related to emergency management planning should be located in close proximity to the ambulance bay. Entrance to these areas should be controlled and restricted to HCF personnel only.

REFERENCES / GENERAL INFORMATION:

ED Violence Surveillance Study, Emergency Nurses Association, Institute for Emergency Nursing Research, August 2010.

The Joint Commission Sentinel Event Alert #4 - Suicide Prevention:

www.jointcommission.org/assets/1/18/SEA_46.pdf

Hospital and Healthcare Security, 5th Ed, Russell L. Colling and Tony W. York, 2010, Butterworth-Heinemann, Stoneham, MA.

SEE ALSO:

IAHSS Basic Industry Guideline 08.02: Use of Video Surveillance.

IAHSS Basic Industry Guideline 09.03: Security in the Emergency Care Setting.

02. Buildings and the Internal Environment
03. Behavioral/Mental Health Areas

STATEMENT:

The design of Behavioral/Mental Health (BMH) patient care settings should address the need for a safe treatment environment for those who may present unique challenges and risks as a result of their medical condition. The BMH patient environment should protect the privacy, dignity, and health of patients and address the potential risks related to patient elopement and harm to self, to others, and to the environment. BMH patient areas should be designed considering the need for considerable clinical and security resources and in accordance with legal and regulatory requirements.

INTENT:

a. This guideline complements the Security Design Guidelines for Healthcare Facilities, Buildings and the Internal Environment Guideline #02.

b. The initial planning and conceptual design phase of BMH patient care settings should include a security risk assessment conducted by a qualified healthcare security professional.

c. The project design team—including the project security representative and those responsible for clinical and operational services within BMH areas—should develop a comprehensive security plan that indicates a layered approach, including zones, control points, circulation routes, and required egress paths. This approach should include the design of security systems to ensure that similar systems or the monitoring of those systems to support clinical operations are addressed.

d. Design should address the variety of HCF settings that may be used in providing care to BMH patients as well as a number of factors impacting where and how care is provided, including diagnosis, gender, age, length of stay, patient acuity, and risk presented to themselves or others. While the level of security will vary based on these factors, standardized design guidelines common to the BMH environment in all HCFs will contribute to the safe treatment of BMH patients.

e. BMH facilities should be designed with a secure perimeter so as to control access to and egress from the facility or unit. Perimeter design should address the following:

   1. Fencing or another type of barrier should surround any external activity areas and these areas should be designed to prevent access to roof areas, the climbing of the fence or building, to limit landscaped areas that may be used for hiding or concealment. A buffer zone of at least 15 feet should be considered between this perimeter and the public. These areas should be designed to provide good observation for staff both in person and via video surveillance to minimize the risks of self harm to patients. Activity areas housed in courtyards should follow the same principles, although fencing and buffer zone requirements may not be applicable.

   2. All exit doors—where deemed appropriate to risk and approved by the local authority having jurisdiction—should be locked at all times. These doors, if locked, will be connected to the fire alarm system and may stay locked when the fire alarm is activated (fail secure) or release on the activation of an alarm (fail safe) based on the patient population and the authority that has

jurisdiction. Alternate entry points to the unit should be available through exit doors for authorized responding personnel only by way of strictly controlled key or card access.

3. Where possible, patient rooms should not form part of the external secure perimeter line.

f. The internal space of BMH facilities should be designed to provide for a safe and secure environment and should consider the following design elements:

1. There should be one primary secure entry to the unit. An intercom (or telephone) and video surveillance for communication to nursing stations from outside the unit should be provided to screen visitors, patients, and staff. The door should preferably be controlled by an electronic access system utilizing an electric strike or electromagnetic lock. The door may be capable of release from the nursing station if visible from that location. The door release button should not be exposed or available to a runaway patient. It should be a constant touch unlocking system where once the hand is removed from the unlock button the door re-locks.

2. In high secure units, or where otherwise deemed appropriate to risk, consideration should be given to installing a double set of secured doors synchronized to prevent both doors from opening at the same time. This creates an elopement buffer zone, which is referred to as a mantrap in some jurisdictions. Consideration should be given to providing a separate staff entry to the unit.

3. Consideration should be given to patient and visitor screening. An area may be provided where patients and visitors are screened for dangerous items and valuables are secured in lockers or other secure space.

4. Visiting areas designed in a location proximate to the main entrance and exit, including a secure area for screening separated from patient treatment areas. Lockers may be provided for visitors' packages, purses, etc.

5. Circulation routes within the unit should be designed for good staff observation, avoiding deep recesses, blind corners, and long corridors that should reduce reliance on video surveillance for observation. The corridors should provide sufficient width so that three people could walk side by side, ideally with high ceilings and constructed with robust deck to deck walls and fixtures installed so as to prevent tampering with mechanical or electrical devices or the creation of a potential weapon.

6. Consideration for areas that are under constant observation such as corridors, education, and therapy rooms or intermittent observation such as bedrooms and washrooms so the design features can be adapted to the frequency of observation.

7. For areas not under constant observation, the prevention of self harm and suicide should be the major factor in design by reducing potential ligature

points and avoiding features that could contribute to self harm.

8. Security of unattended staff and service areas such as maintenance and housekeeping closets, medication rooms, and conference rooms should be designed to be locked at all times and clearly marked as staff areas only. Interview rooms and other rooms where staff may meet with patients one-on-one should be equipped with duress alarms and classroom-type locksets that require a key to lock or unlock the outer handle while the inside handle is always free. Doors to these rooms should be designed to swing into the corridor to prevent entry being barricaded.
9. Patient rooms should be designed so that the entire room is observable from outside the room with light fixtures, fire system components, HVAC grilles and equipment, and window coverings/hardware all recessed or otherwise designed to prevent tampering, reduce opportunity to create weapons, and eliminate aids to self harm.
10. Doors to patient rooms should swing into the corridor if this can be accomplished without creating alcoves that are difficult to observe. Doors should be equipped with classroom-type locks that can always be opened from the inside and the corridor side may be either locked or unlocked with a key.
11. Windows should be safety glazed or equipped with metal screening on the outside and have an opening limited to less than six inches.
12. Furniture should be designed to minimize the possibility of use for self harm as a ligature, as a weapon, or as a barricade.
13. Non-adjustable platform beds, securely anchored in place and with mattresses specifically designed for the BMH environment are recommended. Water and electrical supplies to patient rooms should be able to be isolated by staff from outside the room.

g. BMH design should include safety and security systems that support the maintenance of a safe and secure environment and, when appropriate, monitoring of video surveillance systems to support patient care needs.

1. BMH units should be equipped with duress alarms that can be carried by every staff member working on the unit. Ideally, the device should be capable of transmitting an emergency alarm and receiving information from other alarms. These alarms should be monitored at the nursing station with the system providing specific information on the location of the alarm and, if possible, the name of the person carrying the device. These alarms should also be monitored outside the unit at a control center or switchboard and, where possible, in any immediately adjacent unit.
2. Fire alarm pull stations and fire extinguisher cabinets throughout the BMH area should be lockable and keyed so that all staff on duty are able to access these normally locked devices and cabinets with clearly identifiable keys. As an

alternative, pull station covers that have a loud local audible alarm when the cover is pulled off may be considered.

Sprinkler valves should be recessed in ceiling tile preventing suicide attempt or intentional damage resulting in water damage/evacuation.

3. Video surveillance cameras, in tamper-proof housing, should be utilized in the corridor areas and at the entry and egress points for the unit to provide video surveillance of the unit and activities. The images should be digitally captured and monitored at the nursing station and, ideally, at a control center or security station located off the unit.
4. The nursing station should be designed to maximize the observation of patients while providing confidential areas for staff to work out of sight of patients. Monitors or controls for local cameras should be located at the nursing unit but out of patient view. The height and depth of counter space designed for patient interaction with staff should emphasize staff safety while supporting care and therapy.
5. A designated safe room should be established that can be locked from the inside where staff, patients, and visitors can retreat in the event of an immediate threat or danger. The safe room, in addition to the design for its normal non-emergency use, should be equipped with a telephone, network connectivity, reinforced doors with a peephole installed, duress alarm, and external lock and key access. Consider placing a camera in this room for visual assessment of the area by responding staff members.
6. The medication dispensary and treatment rooms should be housed in two separate but adjacent rooms, observable from the nursing station with a connecting door. The external door to the dispensary should be a dutch door to enable the dispensing of medication, while also preventing patients from entering the room. This door should have an internal shelf on the lower section to assist dispensing and an automatic lock function for the upper section when closed. A deadbolt should be fitted to each of the upper and lower leaves of the door. Drug cupboard doors within the dispensary should be alarmed and all cupboards and drawers should be lockable. Consider the placement of a camera for viewing the drug dispensary area.
7. Communal patient bathrooms or shower facilities should be located within easy access to the patient rooms and be fitted with bath, shower, and sinks of composite material. Items should be designed so as to be as ligature-free as possible or designed to reduce the ligature risk, including lights, bath, shower, and sink controls, mirrors, towel hooks, door knobs, and ventilation grills. Staff should be able to isolate the water and electrical supplies to these rooms from outside the room and all duct work, plumbing, and pipe work concealed. The external door should be fitted with a security lock and occupancy indicator bolt that can be overridden from the outside.

8. Where possible, a BMH unit should have seclusion room facilities so that environmental restraint can be used to support the safe control of patient behavior if necessary. Ideally these rooms should be situated away from other patient rooms and away from regularly patient-traveled corridors, but close to the nursing station. The entry to the room should provide sufficient space for a crisis response team to organize or for a team to manage an aggressive patient as they place the patient in the room. Some key features of the seclusion room include:
9. Door at least two inches thick, outward opening, fitted with viewing window and with a mounting arrangement for door frames capable of withstanding prolonged attack. The locking mechanism should be robust and capable of locking and unlocking quickly from the outside, preferably without a key or access card.
10. Ideally, this room should be a minimum of 130 square feet and should have a stainless steel toilet and sink, with no sharp edges and no ligature aids and designed so that the entire room can be observed from outside the corridor. The ceiling should be at least 9 feet in height and, ideally, the floor and walls designed as one continuous surface.
11. Each room should have tamper-proof mechanical and electrical services fittings with lighting, water, and electrical override controls located external to the seclusion room.
12. The room should be safe for patients and the fixtures and physical details designed and installed so that it would be extremely difficult for a patient to commit suicide or to harm themselves.
13. The room should be equipped with video surveillance cameras preferably with audio capability (check local regulatory requirements and law), and provide a full view of the entire room (even in low light) and situated and designed so as to be out of reach of the patient and protected from tampering or image blocking. The camera image should be digitally recorded and live monitored at the nursing station.
14. The bed should either be a non-adjustable platform bed securely anchored in place with a mattress specifically designed for this environment, or just the mattress itself on the floor of the room. Bedding should also be specifically designed to mitigate the risk of self harm by the patient.

m. For other HCF areas treating BMH patients, these design features should serve as a guide to ensure that patients are treated or continuously observed in a physical environment that reduces the risk of elopement and harm to self, to others, and to the environment.

REFERENCES/GENERAL INFORMATION:

"Design Guide for the Built Environment of Mental Health Facilities," published by the National Association of Mental Health Facilities: www.naphs.org/Teleconference/documents/

DesignGuide4.FINAL.5.24.10_002.pdf

The Joint Commission Sentinel Event Alert #46 - Suicide Prevention:
www.jointcommission.org/assets/1/18/SEA_46.pdf
"Environmental Design Principles – Adult medium secure units" prepared by the Department of Health Secure Services Policy Team (United Kingdom):
www.dh.gov.uk/publications

SEE ALSO:

IAHSS Basic Industry Guideline 09.06: Behavioral/Mental Health (General).

02. Buildings and the Internal Environment
04. Pharmacies

STATEMENT: The design of Healthcare Facility (HCF) pharmacies should address the unique risks presented by the storage and distribution of narcotics and other controlled substances. The design should create a secure physical separation between pharmacy operations and the public while integrating security systems used for access and audit functions. Design considerations should be applied to associated medication distribution points, sub-pharmacies, medication rooms, or offsite pharmacies.

INTENT:

a. This guideline complements the Security Design Guidelines for Healthcare Facilities, Buildings and the Internal Environment Guideline #02.

b. The initial planning and conceptual design phase of new or renovated pharmacy spaces should include a security risk assessment conducted by a qualified healthcare security professional.

c. The project design team—including the project security representative—should develop a comprehensive security plan that indicates a layered approach, including zones, control points, circulation routes, and required egress paths.

d. Risks related to pharmacies are primarily related to:

   1. The products received, stored, controlled, and distributed.
   2. The potential for threats and violence involving personnel and clients.
   3. The potential for internal theft and shrinkage of product.

e. The HCF should design and construct the pharmacy to provide physical security, protect people, and assist in the audit of materials in accordance with policy, regulation, best practices, and assessed risk. The security representative should work closely with the individual responsible for pharmacy operations to implement reasonable and appropriate protection of pharmaceuticals and controlled substances.

f. The HCF should include the design of adjacent space as well as all points of entry from that adjacent space and should include:

   1. The design of pharmacy locations should start with the outer barrier to the space and include penetration-resistant protective measures that extend from solid floor to solid ceiling or roof. This design should prevent access above suspended ceilings through air ducts, cable or utility infrastructure, roof hatches, skylights, unprotected external windows, doors, and dumbwaiters.
   2. Access to HCF pharmacy locations should be restricted and provided through designated doors that provide the following functionality:

      a) Doors that meet or exceed standard commercial grade construction.

      b) Doors that close automatically when not in use.

      c) Doors that automatically lock when closed.

      e) Locking devices that cannot be manually defeated.

      f) Latching/locking hardware that is barrier protected (e.g., astragals, latch guards).

3. Clear and unobstructed view of persons requesting entry and the areas surrounding entry points.
4. Hardening of the transaction window and surrounding wall with protective material that separates public transactions from pharmacy staff. The degree of enclosure and protective material used should depend on the vulnerability as identified in the risk assessment. Ideally, a transaction drawer and security window should have an opening large enough to permit communication and transactions only. A fully opening window should be avoided.
5. Public waiting areas designed within the pharmacy footprint should have secured physical barriers that separate the public from staff work areas. Ideally, dedicated waiting space is not shared with general or clinic waiting space.
6. Pharmacies that are not staffed or occupied on a 24/7 basis should be protected with an intrusion alarm system monitored by an approved monitoring station. These alarms may include, but should not be limited to :
    a) Breach of an exterior entry point, via door position switches.
    b) Breach of exterior openings (exterior or service windows), via glass break or shock sensors.
    c) Activity within the secured space, via motion sensors.
    d) Door(s) held open, via door position switches.
    e) Live or motion-activated monitoring with video surveillance within pharmacy space.

g. The HCF should include the design of integrated security systems to assist in the protection of the staff and the establishment of a safe and secure environment.

1. Systems to control access should be installed at the following locations:
    a) Main Entrance: Staff and others authorized to access the pharmacy should do so through one primary entry point that should restrict access and provide an audit trail of all entries.
    b) Secondary Entrance/Exit: If local code dictates that a secondary entrance be incorporated within the design, access should be restricted and an audit trail of all entries should be recorded.
    c) Pharmacy Receiving: Pharmacy delivery and receiving functions should be channeled through a designated controlled entrance that allows for screening of personnel prior to entry. A video intercom or other mechanism should be installed to allow staff to view and communicate with those requesting access.
    d) Narcotics vault or other controlled substances storage: Access to narcotics storage areas or other controlled substances must be restricted to authorized pharmacy staff and controlled with an additional layer of access control.

2. The HCF should design and construct for operational flexibility around the installation of duress alarm systems. These systems should be installed in areas that allow for staff activation without observation. If installed, systems should be available at strategic staff locations, including transaction windows.
3. Video surveillance should be installed with the specific purpose of recording and digital archiving in accordance with regulatory requirements, institutional policy, or recognized industry best practices. HCFs should consider locating video surveillance cameras at the following locations:
   a) Main perimeter access points.
   b) Receiving areas.
   c) Narcotics vault or other controlled substances storage.
   d) Narcotics refrigerator, if located outside of room vault.
   e) Satellite storage locations.
   f) Transaction counters and windows.
   g) Consideration should be given to the external perimeter of the pharmacy such as connecting hallways, lobby areas, etc. A video monitor should be available to staff inside the pharmacy so they can view the hallway outside the entrance door.
   h) HCF pharmacy locations that do not provide dispensing services to the public should not be identified within the HCF signage program.
   i) Medication dispensing points within the HCF but outside the pharmacy, including, but not limited to, sub-pharmacies, outpatient-specific pharmacies, clinical units, medication rooms, special procedure rooms, and other areas with automated dispensing systems should be equipped with appropriate locking mechanisms, controlled access, and audit systems as described above. Automated dispensing systems design should be integrated with security access system design so that access and audit functionality are consistent. HCFs should consider installing video surveillance to monitor activity at these locations.
   j) Pharmacy functions located outside of an HCF proper, such as offsite clinics and centralized warehousing/distribution centers, will have unique design requirements depending on hours of operation and public interface. When possible, similar design principles to those delineated for HCF pharmacies should be followed.
   k) The design and construction of pharmacy space and security systems should include identification of regulatory and institutional requirements and expectations. Procedures or systems that address access,

audit, security, and the internal operations should be carefully and cooperatively planned by all those who will be involved in the operation and the protection of pharmacy personnel, materials, and space.

REFERENCES/GENERAL INFORMATION:

Hospital and Healthcare Security, 5th Ed, Russell L. Colling and Tony W. York, 2010 Butterworth-Heinemann, Stoneham, MA.

U.S. Department of Justice, Drug Enforcement Administration, Office of Diversion Control: www.deadiversion.usdoj.gov/

SEE ALSO:

IAHSS Basic Industry Guideline 04.04: Drug Diversion.

02. Buildings and the Internal Environment
05. Cashiers and Cash Collection Areas

STATEMENT: The collection, storage, and handling of cash present unique security risks to Healthcare Facilities (HCFs), including design considerations tailored to areas where cash transactions occur or where cash is stored. The design and construction of primary cash management areas should be viewed as a compartment and have a secured physical separation from the public. Security design considerations for primary and secondary cash collection areas should integrate the physical location and layout with security controls and technology.

INTENT:

a. This guideline complements the Security Design Guidelines for Healthcare Facilities, Buildings, and the Internal Environment Guideline #02.

b. The initial planning and conceptual design phase of new or renovated cashiers and cash collection areas should include a security risk assessment conducted by a qualified healthcare security professional.

c. The project design team—including the project security representative—should develop a comprehensive security plan that indicates a layered approach, including zones, control points, circulation routes, and required egress paths.

d. Risks related to cash collection areas are primarily related to the collection, storage, and handling of the cash itself and can pose a risk to the HCF in the event of an armed robbery or internal theft.

e. The design of areas intended for the transaction, handling, or storage of cash or forms of payment should include consultation with a qualified security professional to identify, design, and provide protective measures. This includes cashier offices, financial services, outpatient clinics, cafeterias, gift shops, parking booths, and other areas within the HCF that perform cash or other payment transactions.

f. Access to all doors to the main cashier area should be controlled and restricted to authorized personnel only with audit trail capability. Ideally, the dedicated entrance is limited to one single door.

g. Walls, ceilings, transaction windows, and doors to the cashier office space should be hardened to prevent penetration. The degree of enclosure and protective material used should depend on the assessed vulnerability. Ideally the transaction drawer and security window should have an opening large enough to communicate and perform transactions only. A fully opening window should be avoided.

h. Access to the main cashier area should be restricted and provided through designated doors that feature the following functionality:

   1. Doors that meet or exceed standard commercial-grade construction.
   2. Doors that close automatically when not in use.
   3. Doors that automatically lock when closed.
   4. Locking devices that cannot be manually defeated.
   5. Latching/locking hardware that is barrier protected (e.g., astragals, latch guards).

i. Drop box systems strategically located to facilitate centralized cash collection and protection of cash receipts.

j. Cashier workstations equipped with strategically located duress alarms and recorded video surveillance.

k. Locate safes, vaults, and cash-counting areas outside of the public view. Two-factor identification (dual levels of access control) should be required for entry into such safes, vaults, or areas.

l. Video surveillance should be used to capture and record an image with appropriate detail to identify all persons entering and leaving cashier workstation units. Additional video surveillance should capture images of:

   1. Safe or vault entry.
   2. Cash counting area(s).
   3. Transaction counters and windows.
   4. Satellite cash storage areas outside of the main cashier proper.
   5. Areas where cash is delivered or picked up.

m. Consideration should be given to equipping the cash transaction counter or window with a video monitor displaying live camera images of transactions for public viewing and awareness.

n. Consideration should be given to the installation of video surveillance at the external perimeter of the main cashier office such as connecting hallways and lobby areas. A video monitor should be installed inside the office for staff to view the hallway outside the entrance door.

o. In areas where cash transactions occur or cash is counted or stored, video surveillance should be installed that provides multiple angles of these activities with resolution sufficient for audit or investigation.

p. An intrusion alarm system should be installed and monitored for cash collection areas not staffed or occupied at all times. Consideration should be given to positioning alarm points for the following:

   1. Exterior entry points.
   2. Exterior windows or service transaction counters.
   3. Detecting movement within the secured space.

q. Dedicated public waiting spaces that are compartmentalized with secured physical barriers. Ideally, cashier offices should not share waiting space with general or clinic waiting space.

r. Primary cashier locations often require accessible services at public entrances, but based on the assessed vulnerability may be placed deeper in the facility. The HCF should refrain from identifying cashier locations that do not provide direct service to the public with the way-finding and signage program.

s. Public cash collection areas such as cash registers in the cafeteria and gift shop should include the following design considerations:

   1. Location in an open and visible area.
   2. Unobstructed lines of sight to and from the cashier areas and no blind spots

behind the cashier where the public can observe transactions.

3. Public interaction with cashier designed to minimize public surveillance of cash drawer achieved either through the elevation of the cashier or drawer positioning.
4. Strategically located duress alarms.
5. Recorded video surveillance of the area immediately surrounding as well as all transactions.
6. Consider the use of electronic "smart safes" to ensure large amounts of cash are not on hand in these areas at any time.

x. Public cash collection areas in parking facilities and booths, outpatient clinics, and other areas that may be externally located or isolated within the HCF should include the following design considerations:

1. Cashier workstations that are separated from the public and of sufficient height, width, and strength to make it difficult for someone to jump over, reach over, or physically assault an employee.
2. Unobstructed lines of sight to and from the cashier areas and no blind spots behind the cashiers where the public can observe transactions, cash storage areas, or processes.
3. Strategically located duress alarms.
4. Recorded video surveillance of the surrounding areas and all transactions.
5. Consider the use of electronic "smart safes" to ensure large amounts of cash are not on hand in these areas at any time.

u. The design and construction of cash-handling spaces and cash-collection areas should include identification of regulatory and institutional requirements and expectations. Procedures or systems that address access, audit, security, and the internal operations should be carefully and cooperatively planned by all those who will be involved in the operation and protection of personnel involved in cash collection, cash handling, and cashier operations material and space.

REFERENCES/GENERAL INFORMATION:

International CPTED Association: www.cpted.net

Physical Security Design Manual for VA Facilities: Mission Critical Facilities: www.wbdg.org/ccb/VA/VAPHYS/dmphysecmc.pdf

SEE ALSO:

IAHSS Basic Industry Guideline 09.01 Security Sensitive Areas.

IAHSS Basic Industry Guideline 09.07.Cash and Other Monetary Processing Systems.

06. Infant and Pediatric Facilities

STATEMENT: Healthcare Facilities (HCFs) must address the unique security risks associated with vulnerable patient populations. The design and construction of dedicated infant or pediatric care areas should address the patient and family experience, the physical location and layout, and the integration of security controls and technology.

INTENT:

a. This guideline complements the Security Design Guidelines for Healthcare Facilities, Buildings and the Internal Environment Guideline #02.

b. The initial planning and conceptual design phase of new or renovated infant or pediatric care areas should include a security risk assessment conducted by a qualified healthcare security professional.

c. The project design team—including the project security representative—should develop a comprehensive security plan that indicates a layered approach, including zones, control points, circulation routes, and required egress paths.

d. The design of areas intended to support the care of infant and pediatric patients should include consultation with those who oversee or provide patient care and the security representative to identify, design, and provide protective measures.

e. The project design team should prepare and submit plans to the project security representative for review and approval, including a comprehensive department security plan that indicates zones, control points, circulation routes, and physical security technology locations. This comprehensive security plan should be submitted for review by the security representative prior to submittal to the planning, regulatory, and approval authorities.

f. External entry points to infant or pediatric care areas should be avoided if at all possible and not egress directly outside. Ideally, these unit locations should be positioned above grade or ground level, incorporating controlled-access and code-compliant egress hardware.

g. Access to the infant or pediatric care area should be limited. Access to all doors, interior elevators, and stairwells into the infant or pediatric care area should be controlled and restricted to authorized personnel only. All stairwells and emergency exits serving the infant or pediatric care area should be equipped with delay egress hardware in accordance with applicable codes. Where possible, consideration should be given to a designated staff entry/exit that is separate from public entrances. Relational factors, including movement of personnel and equipment to and from adjoining departments, should be considered when designing the secured compartment (e.g., labor, delivery & recovery, post-partum, NICU).

h. Space should be provided to facilitate a reception process so visitors requesting entry to the infant or pediatric care area can be greeted, positively identified, and screened.

i. Access to service areas should be limited to those directly associated with the infant and pediatric unit. Unrelated areas, functions, and rooms should not be directed through the infant or pediatric unit.

j. All doors leading to the infant or pediatric care area should be equipped with authorized staff-keyed hardware and a clearly marked communication station on the exterior side of the entrance with direct visual observation capability or a video surveillance system to manage the control system.

k. Elevators available to the public should be located outside of the controlled patient care area. Emergency egress paths should be provided for all elevator lobby locations that are outside of the controlled patient care area.

i. Dedicated visitor waiting areas for infant and pediatric care areas should include:

   1. Washrooms and telephones located outside of the controlled patient care area.
   2. Visitor comforts to help with time passage (e.g., television, books and cultural magazines, vending machines, internet access, and age-appropriate toys).
   3. Securely fastened wall hangings, plants, fire extinguishers, or other hard objects.
   4. Recorded video surveillance.

m. Family education or meeting space supporting infant and pediatric care areas should be located outside of the secured environment.

n. All doors to the nursery should be self-closing and secured with controlled access and code-compliant locking hardware.

o. Access to staff lockers and lounges should be secured and controlled at all times and restricted to authorized staff only.

p. Access to supply rooms, medication rooms, clean and soiled linen closets, environmental services storage, and other department function areas should be secured and controlled at all times and restricted to authorized staff only.

q. Video surveillance should be used to capture and record a full-face shot image of all persons entering and leaving the infant or pediatric unit. Additional video surveillance should provide coverage of areas where the public may be allowed to view the nursery.

r. There should be clear lines of sight between unit nursing stations and all public entry points. There should also be clear lines of sight from the nursing station to patient care rooms within responsible care areas.

s. All nursing stations should be equipped with easily accessible duress alarms and video surveillance monitors for all entry/exit points. Consideration should be given to employing a device capable of rapid facility-wide notification of an infant abduction and, if applicable, monitors for the electronic infant monitoring system.

t. Security design considerations for new mother patient rooms that support in-room boarding should include:

   1. Proximity to stairwell exits.
   2. Positioning the mother's bed in the room so that a bassinet can be comfortably placed on the side opposite of the door.
   3. Patient bathrooms sized to accommodate new mother and bassinet placement.
   4. Secure storage for patient valuables and other items of higher value.

u. Consider the implementation of an infant monitoring system as part of the comprehensive security program for infant and pediatric care areas. The system, if installed, should be designed and integrated with the access control system and include:

   1. Controlling elevators that serve the unit (public and staff) to restrict use during an active alarm.

2. Controlling doors to restrict access in and out of the area during an active alarm.
3. Annunciating alarm locally on the unit and remotely to another 24/7 attended location. Local alarm should be loud enough to bring attention to the situation.
4. Positioning a monitor at the nursing station that clearly delineates the location of the alarm.
5. Designing adequate space for zones of warning so they do not impede with patient care and normal movement of patients through the unit (e.g., new mother walking hallways with bassinet).
6. Engaging infant tags actively and routinely to ensure continuous and uninterrupted communication (polling) with the infant monitoring system.
7. Locating system antennae to overlap for an appropriate level of redundancy and the elimination of dead spots.
8. Integrating with the video surveillance system.
9. Securing all control panels in a controlled environment.
10. Verifying that there is no system interference with other electronic devices used in the HCF.

v. Design considerations for pediatric play areas should include:
   1. Access restricted to authorized staff and parents only.
   2. Direct visual observation capability from the nursing station to the play area or a video surveillance system for this purpose.

x. Design considerations for overflow areas and VIP units that house infant or pediatric patients should mirror the newborn maternity level of security.

y. Design considerations for units that mix pediatric and adult patient populations should be assessed for the unique risks that may be present.

REFERENCES / GENERAL INFORMATION:

For Healthcare Professionals: Guidelines on Prevention of and Response to Infant Abductions, Ninth Edition, 2009, National Center for Missing and Exploited Children.

Hospital and Healthcare Security, 5th Ed, Russell L. Colling and Tony W. York , 2010, Butterworth-Heinemann, Stoneham, MA.

International Existing Building Code and International Building Code.

National Fire Protection Association, NFPA 101®: Life Safety Code®, 2009 edition.

SEE ALSO:

IAHSS Basic Industry Guideline 09.02 Infant/Pediatric Abduction Prevention and Response.

IAHSS Basic Industry Guideline 09.09 Pediatric Security.

STATEMENT: The design of Healthcare Facilities (HCFs) should address all forms of confidential patient information commonly referred to as Protected Health Information (PHI). The design should address the multiple ways in which this privileged information can be compromised and should protect that information utilizing integrated physical and electronic security systems. The design should include access and audit systems to be applied, as appropriate, to electronic and written PHI locations in areas, including, but not limited to, registration, interview, clinical, storage, and waste areas as well as within data systems.

INTENT:

a. This guideline complements the Security Design Guidelines for Healthcare Facilities, Building and the Internal Environment Guideline #02 and the Utility, Mechanical and Infrastructure Spaces Guideline #02.08.

b. The initial planning and conceptual design phase of areas that may include PHI should include a security risk assessment conducted by a qualified healthcare security professional.

c. The project design team—including the project security representative and appropriate information security representatives—should develop a comprehensive security plan that indicates a layered approach, including zones, control points, circulation routes, and required egress paths.

d. Risks related to PHI are primarily related to the electronic storage and transmission of PHI, secondary to the physical location of records and ease of viewing or accessing such information, and finally to the destruction of records containing PHI.

e. The HCF should design and construct facilities to provide physical security, protection of information, and to assist in the audit of access to spaces or systems housing PHI in accordance with policy, regulation, best practices, and assessed risk. The security representative should work closely with the individuals responsible for patient records and information technology to implement reasonable and appropriate protection of PHI through the integration of protective measures applied to both physical and electronic spaces.

f. The HCF—in the design of areas that provide patient care, administrative, or other services, and that are open to patients, visitors, and staff—should consider the following for the protection of PHI:

   1. Signage addressing:

      a) Institutional policy or regulation on PHI.

      b) Reminders of the importance of confidentiality (house-wide).

      c) Secure, staff-only or private patient/family areas.

      d) Directions on filling out forms to ensure privacy.

      e) Directions to areas that patients, family, or others should remain while waiting to register, check out, or schedule a future appointment.

2. Registration areas should:
    a) Use systems furniture or other barriers to reduce the opportunity to intentionally or accidently overhear interactions or see registration information.
    b) Include design to reinforce the orderly approach to and from registration desks, such as the use of stanchions.
3. Furnishings should:
    a) Be located in a way to protect computer monitors from public view.
    b) Include hardware to allow for the securing of computers, monitors, etc. to the workstation.
    c) Be designed for the security of records and should include lockable drawers and cabinets.
    d) Include partitions where appropriate to separate workstations or prohibit viewing from open areas.
    e) Include secure receptacles for the pickup, delivery, and distribution of mail/records/film/lab results.
    f) Include space for equipment to be used in the securing or disposal of PHI waste, including secured trash receptacles and shredders.
    g) Locate bed/condition boards in areas that can be viewed by authorized personnel only.
4. Equipment locations should include:
    a) Secure areas for printers, facsimile machines, etc.
    b) Secure pneumatic tube stations if used for the transport of PHI.
    c) Lighting conducive to the use of privacy screens on computer monitors.
5. The HCF, in the design of areas that are primarily used for the storage of health information, including warehouses, record rooms, data centers, or other such locations, should address all points of entry from both public areas as well as adjacent spaces and should include:
6. The design of areas housing PHI should start with the outer barrier to the space and include penetration-resistant protective measures that extend from solid floor to solid ceiling or roof. This design should prevent access above suspended ceilings, through air ducts, cable or utility infrastructure, roof hatches, skylights, unprotected external windows, doors, and dumbwaiters.
7. Access that is restricted and provided through designated doors with the following functionality:
    a) Doors that meet or exceed standard commercial grade construction.
    b) Doors that close automatically when not in use.

c). Doors that automatically lock when closed.

d) Locking devices that cannot be manually defeated.

e) Latching/locking hardware that is barrier protected (e.g., astragals, latch guards).

8. Clear and unobstructed view of persons requesting entry and access to PHI. Areas that include PHI that are not staffed on a 24/7 basis should have security safeguards designed for internal and external monitoring. An intrusion alarm system should be installed and monitored by an approved monitoring station to address alarms, including, but not limited to, the following:

   a) Breach of an exterior entry point, via door position switches.

   b) Breach of exterior openings (exterior or service windows), via glass break or shock sensors.

   c) Activity within the secured space, via motion sensors.

   d) Door(s) held open, via door position switches.

h. The HCF should implement design of integrated security systems to assist in the protection of PHI and the management of a safe and secure environment, considering the following:

1. Access Control systems should be installed at entrances used by authorized staff.

2. Video surveillance should be installed with the specific purpose of digitally archiving in accordance with regulatory requirements, institutional policy, or recognized industry best practices. HCFs should consider locating video surveillance at the following locations:

   a) Main perimeter access points.

   b) Internal areas (without permitting unauthorized viewing of camera monitors displaying PHI).

   c) Consideration should be given to the installation of video surveillance at the external perimeter of areas that are used primarily for the storage of PHI. A video surveillance monitor should be available to staff inside these areas so they can view the area outside of the entrance door.

3. The HCF should consider the design of security technologies that could be applied to both physical and data access control, including two factor applications using keys, passwords, access cards, biometric readers, and other similar technologies.

i. The HCF—in the design of areas housing waste that may include PHI—should utilize access systems and video surveillance systems as described for areas that are used primarily for the storage of PHI (paragraph g., above). Areas that should be considered include:

1. Hazardous waste storage locations (infectious patient waste).

2. Secured waste bin staging areas.
3. Waste disposal treatment areas, if appropriate, housing autoclave, shredders, etc.

j. The design and construction of areas housing PHI should include identification of regulatory and institutional requirements and expectations. Procedures or systems that address access, audit, security, and internal operations should be carefully and cooperatively planned by all those who will be involved in the use and protection of PHI.

REFERENCES/GENERAL INFORMATION:

Hospital and Healthcare Security, 5th Ed, Russell L. Colling and Tony W. York, 2010

Butterworth-Heinemann, Stoneham, MA.

U.S. Department of Health and Human Services Health Information Privacy:

www.hhs.gov/ocr/privacy/

European Commission Privacy Recommendations November 2010:

www.scribd.com/doc/41176451/European-Commission-Privacy-Recommendations-November-2010

Department of Health and Human Services. Centers for Medicare Medicaid Services. HIPAA Security Series. 2005. Web:

www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/physsafeguards.pdf

Department of Health and Human Services. HITECH Act 2009:

www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/hitechenforcementifr.html

STATEMENT: The design of Healthcare Facility (HCF) utility, mechanical, and infrastructure-related space should include the recognition that such space and the mechanical, electrical plumbing, and information technology (IT) systems within it are critical assets for the HCF that provide for uninterrupted patient care, basic building comfort, and extraordinary emergency response capabilities.

INTENT:

a. This guideline complements the Security Design Guidelines for Healthcare Facilities, Parking and the External Campus Environment Guideline #01 and Buildings and the Internal Environment Guideline #02.

b. The initial planning and conceptual design phase of new or renovated utility, mechanical, and infrastructure space should include a security risk assessment conducted by a qualified healthcare security professional.

c. The project design team—including the project security representative—should develop a comprehensive security plan that indicates a layered approach, including zones, control points, circulation routes, and required egress paths.

d. The design of utility, mechanical, and infrastructure-related space, given its critical nature, should include facilities and security expertise as well as representation from administration, safety, clinical departments, IT, emergency management, and other stakeholders whose operations rely on utilities, building systems, information, and communications infrastructure.

e. The HCF should design and construct to provide security protection and emergency response for critical utility systems. The HCF should:

    1. Identify and provide protective measures to areas in which utilities, including water, steam, electrical power, communications, compressed gases, and chilled water are produced or distributed in order to minimize the opportunity for disruption of those services.

    2. Identify and provide protective measures to areas in which backup utility systems, including generators, clean steam boilers, gas canisters, and other redundant systems are located. These measures apply to areas designated for the storage of fuels used to power backup equipment.

    3. Design for emergency response to loss of utilities and should include separate means for redundancy in the delivery of purchased utilities, including gas, water, steam, electrical power, telecommunications, and other information technology services.

    4. Allow for the alternate delivery of utilities (as described in item 1, above) through the construction of access points into internal distribution systems in case services are needed from portable boilers, generators, gas tanks, etc.

    5. Design access roads, driveways, etc. to allow for the delivery of fuels or alternate utility generation (as described in items 2 and 4, above).

6. Provide that utility and infrastructure design and construction plans complement and support institutional continuity of operations/business continuity planning objectives.

f. The HCF should integrate security measures into the design of mechanical and critical infrastructure spaces in order to provide for a work environment in which major systems are secure from unauthorized access. The HCF should:

   1. Limit access to personnel that manage and maintain the mechanical, electrical, HVAC, and plumbing systems. This should include, but not be limited to, electrical vaults, elevator machine rooms, water supply systems, and air handler intakes.
   2. Limit access to data centers, areas that house servers and other hardware, and areas where systems are monitored, including, but not limited to, information technology, telecommunications, and building automation and security systems.
   3. Limit access to rooftops in the same manner as for mechanical, electrical, and plumbing system spaces, including roof access hatches as well as doors leading from secured mechanical spaces.
   4. Design storage areas within the mechanical space for use by those who have access and secure such storage facilities within the larger area.
   5. Incorporate similar security designs with regards to telecommunications, information technology, security, fire alarm, and building automation rooms or spaces throughout the building. Panels serving these systems should be secured and may be alarmed.
   6. Secure rooms or spaces storing plans allowing for access by both internal and external emergency responders.
   7. Include detailed utility and mechanical system plans within mechanical or technology rooms for use by security, facilities, or emergency response personnel from within the organization or from public responders.

g. The HCF should design and build infrastructure to provide for redundancy and potential expansion as it relates to the growth of technology and the subsequent demand on utility and mechanical systems that may require enhanced security or other building systems. The HCF should:

   1. Incorporate the design and construction of stacked technology rooms when possible to allow for the easy management of cables and wire related to security systems, telecommunications, information technology fiber, building automation, fire alarm connections, and the efficient use of networked systems.
   2. Integrate security systems infrastructure into the design and engineering of the project to ensure that there is space for current and future panels related to the systems designated above and to allow shared uninterrupted power supplies and the appropriate environmental needs as the technology evolves.

3. Consider the potential increased need for mechanical, electrical, and plumbing capacity when designing infrastructure so that services can be provided in the event that clinical technology requires more electrical power, air conditioning, or higher levels of security.
4. Provide network capabilities for current need and anticipated growth in security systems or for the future implementation of those systems.

REFERENCES/GENERAL INFORMATION:

Telecommunications Industry Association (TIA) 1179 Healthcare Facility. Telecommunications Infrastructure Standard.

National Fire Protection Association, NFPA 730: Guide for Premises Security.

STATEMENT: Healthcare Facilities (HCFs) should address the unique security risks presented by highly hazardous materials (HHMs), including, but not limited to, biological, chemical, and radioactive materials and should be aware that areas housing HHMs are frequently regulated and must be designed accordingly. HCFs should design and construct to provide integrated physical security, the protection of the internal and external environment and the surrounding community, and to assist in the audit of materials in accordance with policy, regulation, best practices, and assessed risk.

INTENT:

a. This guideline complements the Security Design Guidelines for Healthcare Facilities, Parking and the External Campus Environment Guideline #02 and Buildings and the Internal Environment Guideline #03.

b. The initial planning and conceptual design phase of new or renovated biological, chemical, or radioactive materials use space should include a security risk assessment conducted by a qualified healthcare security professional.

c. The project design team—including the project security representative—should develop a comprehensive security plan that indicates a layered approach, including zones, control points, circulation routes, and required egress paths.

d. The design of areas intended for hazardous materials use, storage, or disposal should include the security representative as well as those from facilities, safety, environmental health, and others responsible for the management of HHMs to identify, design, and provide protective measures.

e. Areas to be addressed include, without being limited to, the following:

1. Laboratory spaces with special attention to Biosafety Level-3 (BSL-3) and above laboratories; Select Agent laboratories (if applicable); laboratories using radioactive materials, highly hazardous chemicals, controlled substances, and material storage areas within those laboratories.
2. Patient care areas that use HHMs such as radiopharmacies, nuclear medicine facilities, or radiation treatment areas.
3. Storage or disposal areas used for the management of pharmaceutical hazardous waste.
4. Waste storage areas housing infectious waste, radioactive waste, and chemical waste to ensure the management of access for both authorized employees and vendors, if applicable.
5. Spaces housing gamma irradiators or other devices containing significant amounts of radioactive material.
6. Facilities storage, mechanical space, and grounds maintenance areas involving the use, storage, or distribution of hazardous materials.

f. Design of locations housing HHMs should be segregated by type of waste, include penetration-resistant protective measures that extend from solid floor to solid ceiling or roof, and prevent access through air ducts, cable, or utility infrastructure, through roof hatches or skylights, or through unprotected external windows or doors.

g. Access to locations that may be used for work with—or storage or disposal of—biological, chemical, or radioactive materials should be restricted, and include hardware for automatic closing and barrier-positive latching that operates and secures the door when in the closed position.

h. Security safeguards should be designed for internal or external monitoring. An intrusion alarm system should be installed and monitored by an approved monitoring station to address alarms, including, but not limited to, those activated through video surveillance, door position switches, and motion sensors.

i. Where appropriate, video surveillance should be installed for the purpose of digitally archiving activities in accordance with regulatory requirements or recognized industry best practices.

j. Rooms or areas should be designed to address risks associated with HHMs, including, without being limited to, exposures that may cause illness, chemical reactions that may lead to fire, explosion or the creation of dangerous gases, changes in pressurization or level of oxygen in a space, and other potentially dangerous situations.

k. Rooms or areas associated with HHMs should be monitored or managed using access, audit, construction, ventilation, detection, fire suppression, and building/equipment alarm systems.

l. Considerations for both internal and external emergency response should be included in the design of space that may be used for work with HHMs, including:

    1. Location of space that has appropriate building systems, including adequate ventilation systems (negative pressure, direct exhaust, etc.), adequate electrical service, fire suppression systems, and appropriate utility backup systems.

    2. Locations external to the space for emergency response equipment, personal protective equipment, decontamination protocols, access and egress for internal and external responders, area for space, and systems plans, if needed during response.

m. The hazards associated with HHMs are frequently addressed in international, national, and local regulations, guidelines, or standards. These standards define risk assessment-based approaches to developing safe, secure facilities that control, audit, and dispose of such materials in accordance with those documents. The Security Representative should work with those facilities that use highly hazardous materials and with Facilities and Administration to research and understand the risks, requirements, and best practices in this area.

REFERENCES/GENERAL INFORMATION:

IAHSS Directions Article, DOE Program Offers Hospital Security Training and Resources for Securing Radiological Materials from Terrorists, Volume 23, Number 4, 2010, Page 35–36.

www.iahss.org/DIRECTIONS/directionsdec2010.pdf

International Building Code, 2009, Section 415, Groups H-1, H-2, H-3, H-4, H-5.

http://publicecodes.citation.com/icod/ibc/2009/index.htm

Biological

U.S. Select Agents Regulations (42 CFR Part 73, 7 CFR Part 331, 9 CFR Part 121).

www.selectagents.gov/Regulations.html

Biosafety in Microbiological and Biomedical Laboratories (BMBL) 5thEdition from Centers for Disease Control and Prevention (CDC).

www.cdc.gov/biosafety/publications/bmbl5/

World Health Organization Laboratory Biosafety Manual:

www.who.int/csr/resources/publications/biosafety/Biosafety7.pdf

Chemical

U.S. Department of Homeland Security Chemical Facility Anti-Terrorism Standards (CFATS): www.dhs.gov/files/laws/gc_1166796969417.shtm

World Health Organization International Programme on Chemical Safety (IPCS):

www.who.int/ipcs/en/

Resource Conservation and Recovery Act (RCRA):

www.epa.gov/region1/enforcement/waste/rcraregs/adeq.html

Radioactive

U.S. Nuclear Regulatory Commission Security:

www.nrc.gov/security/byproduct/orders.html

Global Threat Reduction Initiative:

http://nnsa.energy.gov/mediaroom/factsheets/reducingthreats

International Atomic Energy Agency Code of Conduct on the Safety and Security of Radioactive Sources: http://nnsa.energy.gov/mediaroom/factsheets/reducingthreats

03. Emergency Management

STATEMENT: The design of the Healthcare Facility (HCF) should consider emergency management practices that allow for the flexibility and resilience required to manage emergency events. An all-hazards approach to design should be applied to help the HCF prepare for, respond to, and recover from manmade events and natural disasters.

INTENT:

a. This guideline complements the Security Design Guidelines for Healthcare Facilities, General Guideline, Parking and the External Campus Environment Guideline #01 and Buildings and the Internal Environment Guideline #02. Design Guidelines #02.02 Emergency Departments, #02.07 Utility, Mechanical and Infrastructure and #02.08. Biological, Chemical, Radiation Use Restricted Areas also have considerable interface with this guideline.

b. The initial planning and conceptual design phase of construction and renovation projects should include a security risk assessment conducted by a qualified healthcare security professional and the appropriate clinical, facilities, and other support personnel with responsibilities related to emergency management. A Hazard Risk Vulnerability Assessment should be completed by those responsible for emergency management for the HCF.

c. The project design team should prepare and submit plans to the project security representative for review and approval, including a comprehensive emergency management plan that complements the layered approach to design that is described in the guidelines referenced in Intent (a., above).

d. The design should support the ability of the HCF to shelter-in-place and repurpose space during emergency operations to accommodate the intake and care of a surge of patients. This should include consideration for:

   1. Assignment of patient care populations to avoid evacuation complications based on mobility of patients.
   2. Mass triage during such events as epidemic or pandemic outbreaks.
   3. Increased inpatient capacity.
   4. Increased isolation capacity, including installing medical gasses and other necessary patient care elements in walls and ceilings of rooms intended to be dual-use, convertible space.
   5. Staging area(s) for emergencies.
   6. Community support related to widespread utility outages or severe weather conditions.
   7. External areas for supplies or other support vehicles or trailers.
   8. Areas for permanent or temporary helipad facilities.
   9. Increased morgue capacity, including racks for storage and cooling capability.

e. The design should include consideration for the following in preparation for response to emergency situations:

1. Alternate points of access:
    - a) Exterior doors that could be used as alternate entrances to temporary treatment/triage areas should be designed to allow for emergency access.
    - b) External design should provide for clear access to alterative emergency entrances.
    - c) External access paths addressing personnel, vehicles, parking, staging, and emergency patient transport needs should be considered as related to the use of alternate entrances and the care provided in reassigned spaces.
2. Space reassignment:
    - a) Internal design should allow for the repurposing of space used for emergency response by addressing controls to and from that space. This may include controlled access systems, fire doors, and fixed furniture design.
    - b) Areas considered for alternate care sites should include additional electrical infrastructure to accommodate patient care equipment and other required services.
    - c) Design consideration should be given to allow for curtains or other such privacy apparatus in areas considered for alternate care or reassignment.
3. Permanent or temporary emergency support space should include appropriate access to electrical and information technology infrastructure, and include:
    - a) Design of an Institutional Emergency Operations Center that includes access to video surveillance, intrusion detection, access control, utility, fuel, and building systems and can be activated as needed and to the degree (scale) necessary to respond to emergencies at all levels.
    - b) Designation of space that could be reassigned to serve as an Emergency Operations Center for external responders.
    - c) Designation of space to support patient care functions, including triage, operating and patient room assignment, and discharge and morgue management.
4. Designation of space to provide services and support to large numbers of individuals in areas preferably separated from patient care and emergency management areas, as described above.
    - a) Designation of space to accommodate families.
    - b) Designation of space to accommodate mental health support.
    - c) Designation of space to accommodate media.

5. Designation of space, external to the buildings, to serve as assembly and staging areas and the ability to separate that space from other external space when needed.

f. The design of the HCF should include a risk assessment, including the impact of wind on the HCF site. The construction or renovation of space should include built measures to mitigate risks identified in that risk assessment and should include consideration for the following design-related measures:

1. Critical utility supply addressing power, steam, gas, and water are delivered or located in areas least vulnerable to sabotage or natural disaster and that, if purchased from external providers, access to such infrastructure is controlled within HCF property.
2. Critical infrastructure such as generators, water and fuel storage, and mainframe computer systems are also located in areas least vulnerable to sabotage or natural disaster.
3. The ability to quickly manage the environment, including the ability to:
   a) Lock down the HCF and isolate all access and egress to select locations.
   b) Manage air intakes so that they can be shut off immediately when necessary.
   c) Control air circulation by management of heating, ventilation, and air conditioning and related filtration systems in the event of an emergency that requires the isolation of areas, purging of the system, or reversal or air flow.
6. Systems that have both primary and secondary (backup) capabilities should be included in the design and the primary and secondary delivery should be designed as separated redundant systems to eliminate single points of failure.
7. System redundancy should be designed in accordance with applicable institutional standards, best practices, and regulatory requirements and should, within an HCF environment, minimally address safety and comfort in:
   a) Patient care systems and space.
   b) Lobbies and other large gathering areas.
   c) Life safety systems and egress paths.
   d) Building automation, information technology, security, and telecommunications systems, including local panels, cameras, alarms, access readers, radio repeaters, and wireless access points.
   e) Data centers.
   f) Dispatch and system monitoring areas.
   g) Emergency operations centers.

8. The design of systems that can be supported from outside the HCF or that impact the external environment should include:
    a) The installation of quick connects for portable utility backup systems.
    b) The installation of air intakes above ground level.
    c) Construction that addresses exterior walls, windows, and other elements to protect the building from natural and man-made disasters.
    d) Review roof top systems as they may be impacted by wind or other weather conditions.

g. Continuity of Operations design should include consideration for:
    1. Space to accommodate storage of supplies of food, water, pharmaceuticals, and other supplies necessary to ensure that the facility can be self-sufficient for the recognized best practice standard of 96 hours. This amount of time may be adjusted based on institution-specific needs.
    2. Space to relocate administrative staff should primary administrative facilities be converted to triage/patient care space.
    3. Backup systems space for data center management.
    4. Respite areas for sheltering staff.

h. Building names or numbers should be placed in a highly visible area of the building to assist emergency responders with campus location orientation.

i. Decontamination areas should be located on the outer perimeter of the building. Design elements should include:
    1. Exterior entrance for decontamination shower rooms that is controlled and restricted to authorized staff only and protected from weather and wind elements.
    2. Space to house personal protective equipment for decontamination team.
    3. Dedicated holding tanks to accommodate decontamination run-off.

REFERENCES/GENERAL INFORMATION:

Physical Security Design Manual for VA Facilities: Mission Critical Facilities: www.wbdg.org/ccb/VA/VAPHYS/dmphysecmc.pdf

Best practices of hospital security planning for patient surge--a comparative analysis of three national systems: www.ncbi.nlm.nih.gov/pubmed/20873500

SEE ALSO:

IAHSS Basic Industry Guideline 10.01 Emergency Management (General).

IAHSS

International Association for Healthcare Security & Safety

P.O. Box 5038, Glendale Heights, IL 60139

(888) 353-0990 • www.iahss.org