

RISK MANAGEMENT IN HEALTH CARE INSTITUTIONS

LIMITING LIABILITY AND ENHANCING CARE

THIRD EDITION

Florence Kavalier, MD, MPH, MS
Raymond S. Alexander, MBA, MS

Chapter 7: Assuring Safety and Security in Healthcare Institutions

Safety and Security – Risk?

- Health facilities that experience adverse events due to safety or security issues can incur penalties ranging from large fines to loss of accreditation.
- An aggressive and well-organized safety and security management program can help minimize risk of and adverse event.

Regulation and Accreditation

- Medicare and Medicaid require a participating healthcare organization to satisfy the Conditions of Participation (CoP) relevant to the management of safety and security.
 - Accreditation by the Joint Commission, DNV Healthcare Inc. or HFAP ensures that the facility meets the CoP requirements
- State Departments of Health also regulate safety and security in healthcare organizations

Safety vs. Security

- Safety can be a broad category with standard policies and procedures throughout a facility or system.
 - Hand-washing policy
 - Use of Personal protective gear
 - Hazardous waste disposal
- Security must be more site specific.
- Safety and security policies sometimes conflict.

High Risk Events

- A facility may incur major penalties if a “never” adverse event occurs (an event that should not occur if appropriate safety/security measures were in place)
- CMS may not reimburse costs of a never event and many third party payers have a non-reimbursement program as well.

Techniques for Managing Safety and Security

- Risk Assessment Estimate
- Failure Modes and Effects Analysis (FMEA)
- Root-cause Analysis (RCA)
- Technological Redundancy
- Crew Resource Management
- Red Rules

Potential Environmental Hazards

- OSHA has a list of the types of hospital-wide hazards and provides information on how to prevent and respond to them
- Three categories of hazardous materials
 - Biological
 - Chemical
 - Radioactive

Security: Unwanted Intruders

- Use of high-tech solutions to manage visitor and employee access
 - Automated turnstiles with card swipe readers for employee entrances
 - Visitor areas/desk where all visitors enter and sign-in.
 - Employee ID badges
 - Secured areas

Potential Security Hazards

- Theft of Patient Valuables/Employee theft
- Infant abduction
- Workplace Violence
- Gangs

Patient Valuables

- Provide a safe in the building to house valuables
- Provide receipts for any valuable stored by facility
- Encourage patients to leave valuables at home or give to family to take home

Violence in the Workplace

- Patients have a right to treatment but staff have a legal right to a safe workplace
- Watch for signs that may lead to violence (in patients, visitors and staff)
 - Anger
 - Stress
 - Under the influence of drugs/alcohol

Gangs

- Many health facilities treat victims of gang violence and occasionally the dispute continues upon arrival at the facility.
- Use of metal detectors is increasing to prevent entrance of weapons into the health facility

Information Security

- With increasing use of information management systems, healthcare facilities must insure that the system itself is secure from unauthorized access or violate HIPAA regulation
 - Entry to system is password or thumbprint protected
 - Use of firewalls to block unauthorized internet access
 - Use of Virtual Private Networks

Fire Safety

- Health facilities must comply with NFPA standards for fire suppression systems, fire barriers, smoke compartments, detectors and alarms, and emergency exits and lighting
- Defend in Place
- Fire Safety Plans and Training

Facility Design and Operation

- The design of the physical plant can help ensure safety and security of the facility
 - Proper ventilation design can ensure indoor air quality and safety
 - Use of improved technologies to keep water clean and prevent growth of bacteria
 - Use of technologies to prevent scalding from high water temperatures

Emergency Preparedness

- Dedicated resources for emergency preparedness
- Designation of a command structure
- Culture of continuous training
- Frequent and critiqued disaster drills
- Constant updating of plan to reflect changing risk and conditions

Types of Threats

- Security
- Utility Failures
- Geologic
- Structural
- Other

Plan for Information System Continuity

- As healthcare organizations rely more heavily on information technologies, it is imperative that there be a specialized disaster plan for information technology.
 - Backup data systems
 - Independent emergency power supplies
 - Alternative network communication

Summary

- Safety and security incidents can be serious threats to the financial well-being of the healthcare organization.
- The Risk Manager must be aware of potential safety and security situations and ensure policies and procedures are in place to minimize the risk of an incident.