HOSPITAL NOTES

Security risks / Vulnerabilities V/s Security Tactics to Prevent Loss in Hospitals

Yashpal Sharma*, Jasbir Singh**

Introduction

In the olden days the hospital enjoyed a kind of unspoken immunity to the nasty sites of crime, violence to the patients or staff, thefts, fraud and embezzlement etc. But the scenario has now changed and the hospitals have become more tempting targets for crime and theft and the reason being that the hospitals contain very expensive equipments, large quantities of drugs and chemicals in the stores. A wide range of retail goods are stocked in hospital shops and even cash is kept in the cashiers room.

Similar changes have occurred in other organisations also but they have been able to respond to the pressures of rising crime by altering their working practices. In the hospitals the situation is entirely different as the activities keep on going at varying intensity through out the 24 hrs. of a day, with unforeseeable peaks, so there are large no of people in and around the hospital all the time, and the hospital has to be flexible and sensitive.

Hospital Security is "a system of safeguard designed to protect and to achieve safety of the patients, public, hospital personnel and property and also to achieve relative safety for all people interacting within the hospital and its environment".

The safety has to be in relative terms as what is safe today may not be safe tomorrow.

Need for Hospital Security

(i) **"Moral Responsibility"**: To minimise the possibility of injury or death and also to take reasonable steps to preclude the destruction, misuse or theft of property.

(ii) **"Legal Responsibility"**: The hospital's obligation to its patients is contractual and especially for critically ill patients, psychiatric patients, elderly and the infants.

(iii) A tool for maintaining good **"public and employees relations"**.

Objectives of Hospital Security

(i) Protecting patients, visitors and employees from harm and its reasonable fear.

(ii) Protecting personal and hospital property from theft, misuse, or vandalism.

(iii) Maintaining an acceptable level of order, control and safety in various hospital buildings and departments.

(iv) Enforcing various hospital's Rules and Regulations.

*Deputy Medical Supdt., District Hospital, Udhampur, **Medical Supdt., Govt. Medical College Hospital, Jammu J&K.
Correspondence to : Dr. Yashpal Sharma, Deputy Medical Superintendent, District Hospital, Udhampur, J&K India.

SECURITY RISKS VULNERABILITIES

1. **Assaults :** These may occur between :

   (a) Patient and Staff.
   (b) Staff and Visitors.
   (c) Patients.
   (d) Family members.
   (e) Staff members.

   The Hospital Emergency department and psychiatric treatment areas witness the frequent scenes of assault.

2. **Burglary :** The numerous targets for hospital burglaries are :

   (a) Places where cash is stored.
   (b) Operating rooms.
   (c) Store room.
   (d) Work areas/wards
   (e) Office areas and so on.

3. **Destruction of Property (Vandalism) :** This ranges from writing on the walls, sticking posters to complete shutdown of facilities. The disgruntled employees and employee unions are the prime cause of these malicious acts.

4. **Disturbances :** The internal disturbances involving patients, visitors and employees are quite common in almost all the hospitals. These range from verbal arguments to assaults and destruction of property. The common area for disturbances are OPDs and Emergency Department.

5. **Drug Abuse :** This has been increasing alarmingly over the past few years. Narcotic addiction amongst the doctors and other hospital staff is much more serious problem than is generally recognised.

6. **Homicide and Suicides :** These are very common in psychiatric wards & sometimes even employees can resort to homicides.

7. **Imposters :** Impersonating as employees, staff, nurses, physicians etc. is another security vulnerability that occurs with a high degree of frequency.

8. **Kickbacks and Frauds :** Many forms of kickbacks, frauds and embezzlement occur in almost all medical care organisations. Insurance frauds, fraudulent claims for reimbursement, kickbacks for the purpose of medical equipment are all quite common in a hospital setting. An effective security system will reveal embezzlement before it becomes disastrous.

9. **Kidnapping :** The threat of abduction is generally associated with the new born and paediatric patients.

10. **Loss of Information :** The loss of confidential or privileged information is a security vulnerability that is often overlooked in medical clinics and hospitals. The medical records of the patients are of prime importance.

11. **Strike/Mass Casual Leaves :** These create the following problems

    (a) Disruption of services from within.
    (b) Disruption of external services.
    (c) Malicious destruction of facility, owned property and the personal property of employees.
    (d) Intimidation and assault on pro-management employees.
    (e) Harassment in general.

12. **Safety related Vulnerabilities :** These can be briefly listed as under :

    (a) Accident due to :

    - Unsafe physical facilities / conditions.
    - Inadvertent act of victim.
    - Inadvertent act of another person.

    (b) Fires : These may be :

    - Accidental

- Due to arson

(c) Internal or External Disasters.

13. **Thefts :** The thefts of supplies, equipment and personal property is common to all health care organisations. The specific loss of any hospital is very difficult to calculate and is like tip of an iceberg, only a small part of the problem actually surfaces. The theft may be of :

- Hospital property
- Staff or patient property

14. **Pilferage in Hospital :** "Pilferage means small scale theft of insignificant items", but regular or long term pilferage, if neglected can add up to a major loss.

"A security guard in the front door is a folly if the backdoor is neglected. The amount of money lost through the front over a ten years span will in no way match the loss you suffer in one year through the back doors".

The following material is most vulnerable to Employee pilferage

(a) **Linen :** Sheets, towels, blankets, curtains, draperies etc.

(b) **Clothing :** Uniforms, aprons, robes and gowns.

(c) **Food :** patient's trays, cafeteria and dietary department supplies.

(d) **Maintenance supplies :** paint, hardware, light bulbs, plumber and power tools, plumbing supplies.

(e) **Paper goods :** Stationery, office supplies, house keeping supplies.

(f) **Capital Equipment :** Electric fans , Projectors, Typewriters, Computers, printers, furniture etc.

(g) Drugs & pharmaceuticals .

(h) **Money :** Hospital and personal

(i) **Patients and Employee's belongings :** Jewellery, luggage, clothing, personal appliances.

(j) **Medical supplies and Equipment :** Stethoscope, Surgical instruments, Lab equipments.

(k) **Gift Shop supplies and Equipment.**

(l) **Photographic Supplies equipment.**

(m) **Housekeeping Supplies :** Soaps, brooms etc.

(n) **Time :** Intangible but very costly & so on.

SECURITY TACTICS TO PREVENT LOSS IN HOSPITALS

It is usually a mistake to place the primary responsibility of preventing loss of hospital assets on the security chief. He can essentially contribute in the area of perimeter protection, internal lock up effectiveness, traffic control in all its dimensions and investigative activities, including contact with law enforcing agencies. A person well versed with problems of the material handling, paper work documentation and accounting procedures would be a logical choice. *A person with police/belt forces background or experience of other law enforcing agencies should be a preference.*

There are three elements to a criminal act :

(a) **Motive :** The motive can be corrected by morale building, fear and effective programmes.

(b) **Means :** Means can be checked by routine cheeks at various exists and limiting access to high risk areas. These measures are of minimal effect for internal thefts.

(c) **Opportunity :** Opportunity is the only control level element.

The Hospital employees or people who have the most opportunities :

(i) Supervisors and Authority figures.

(ii) Guards
(iii) Night and weekend employees who are generally unsupervised for long periods.
(iv) Staff with keys.
(v) Long term trusted employees
(vi) Store Keeper and Receiver.
(vii) Clerks handling money & pay rolls or equipment records.
(viii) Service department personnel
(ix) Terminated employees.

STRATEGIES TO MINIMISE THE OPPORTUNITIES

- Minimum doors should be kept open after office hours.
- All employees be given photo identity cards & uniforms for certain groups.
- Visitor passes to be provided & visitors in excess number should be discouraged.
- Proposed visiting hours for visitors with pass and general visitors should be strictly followed.
- Traffic Control in the Hospital.
- Alarm System in the Hospital to alert the security personnel.
- 24 hrs. internal security guard coverage in the hospital which can prevent petty pilferage by checking and controlling at each level.
- Patients should be advised not to bring any valuables in the hospitals.
- Locking of the hospital/department doors should be done by the nominated persons on roster duty.
- Key should be deposited in the security office, where time of deposit and name of person who deposited the keys should be entered. The signature must also be obtained at the time of issue of the keys.
- Duplicate keys should be kept in a bag which should be sealed with two signatures of officasis from different offices.
- Good quality of the locks should be used and if key is lost, it is advisable to buy a new lock and replace the other immediately.
- Duty rosters of guards & supervisors should be prepared twice in a week to ensure that same person is not given the same duty through. There should be proper handing over and taking over at the end of the duty.
- Maximum lights should be provided in the hospital premises. All electrical appliances not in use at night shall be put off & water taps should be properly closed to prevent fire and floods respectively in the rooms, which may destroy the equipment /files/ documents.
- All out going and incoming items (Which are taken in the hospital for personal use like TV, Coolers) must have a gate pass from the security officials.
- All medical equipments like microscopes, ophthalmoscopes, endoscopic equipment and office equipment like typewriters, Computers etc. should be kept in lock and key and accountability must be fixed to some employee for taking care of these equipments.
- In case any person found guilty of theft, should be handed over to the police & debarred from entering hospital.
- Security department is also responsible for fire safety in the hospital. So regular drills, frequent checking of fire hydrant system, fire extinguishers should be conducted & hospital must have a fire manual for effecting functioning.
- The use of security audits and documents control has proved highly effective. Management must monitor long term relationship between house purchasing officials and the suppliers.

References

1. John E. Guide to Hospital Security: Grover Publishing Co. Ltd. England (1983).
2. Safety Manual: American Hospital Association: Chicago. Ellinois (1988).