AHPI
HOSPITAL SAFETY & SECURITY MANUAL









OCTOBER 2024

AHPI HOSPITAL SAFETY AND SECURITY MANUAL

Prepared by:
AHPI Task Force

ASSOCIATION OF HEALTHCARE PROVIDERS INDIA

CONTENTS

Serial No.	Topic	Page No
1	About AHPI	4
2	Foreword	5
3	Composition of the Task Force for Developing	6
4	Introduction	7
5	Security Policies	9
6	Security Personnel	29
7	Access Control	41
8	Surveillance System	45
9	Incident Response	49
10	Physical Security Measures	55
11	Cybersecurity	67
12	Handling Specific Threat	79
13	Coordination With External Agencies	97
14	Annexure-1	107

ABOUT AHPI

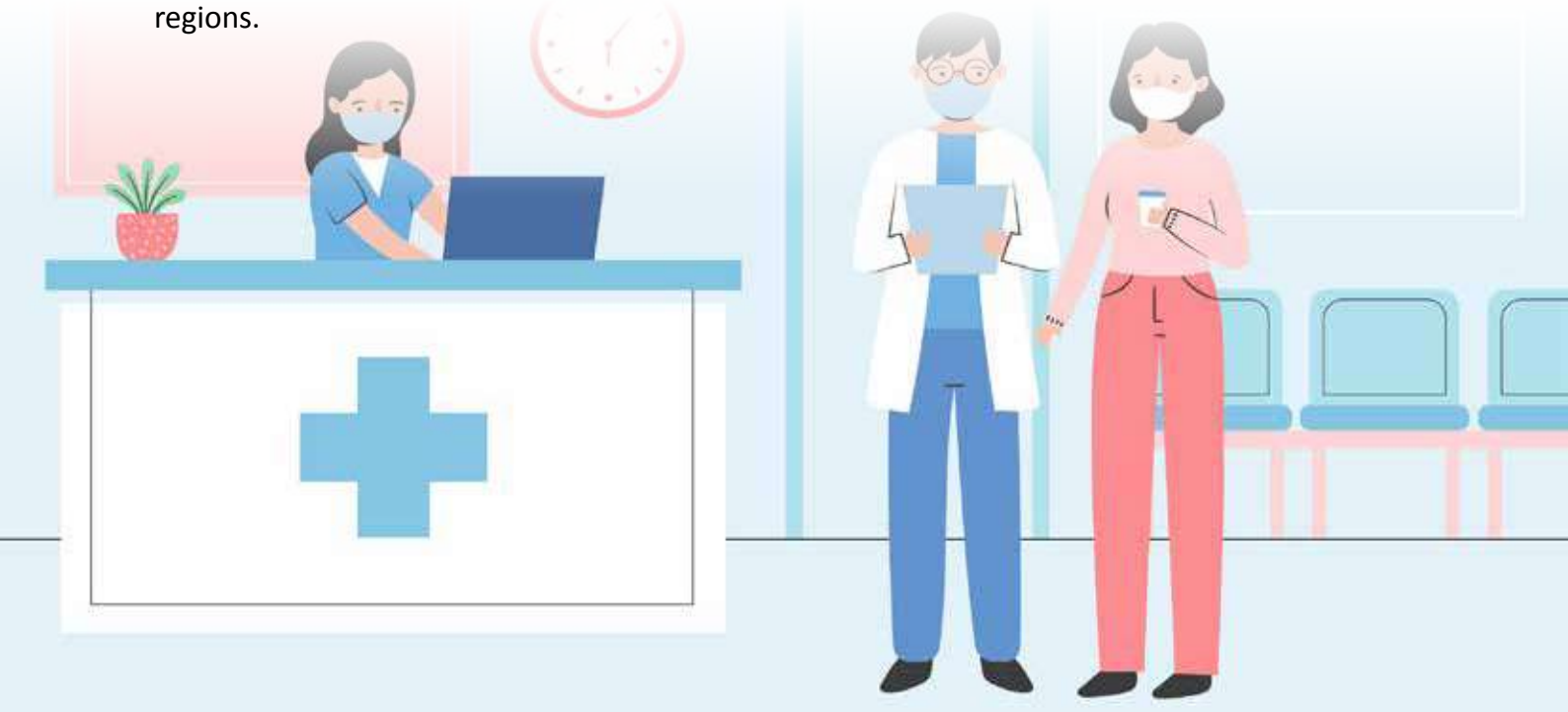
Association of Healthcare Providers (India) represents the vast majority of healthcare providers in India. It is registered under Indian Society Registration ACT- 1860 as “not for profit” organization.

The Association of Healthcare Providers (India)’s vision is to have healthy India, encompassing society, community and common man at grass root. The Association of Healthcare Providers (India) envisions a healthy India, with a focus on improving the well-being of society, communities, and individuals at the grassroots level. AHPI collaborates with all key stakeholders to establish a national healthcare system that ensures universal access to essential health services for every citizen.

AHPI supports its members and partner organizations in driving healthcare improvements that benefit communities effectively and efficiently. It plays an active role in advocating for healthcare reforms, infrastructure development, tax and tariff regulations, health insurance issues, and any other challenges that healthcare organizations or the public face in delivering or accessing equitable healthcare services.

Through its subsidiary wings, the AHPI Academy, the association offers various healthcare programs that prioritize patient safety and quality of care. Another important entity under AHPI is the Healthcare Certification Centre, which develops standards for different categories of healthcare establishments. It also certifies healthcare agencies’ compliance with these standards and provides customized, certified training programs, including Quality Management System (QMS) and healthcare management training for the industry.

In a relatively short span, AHPI has become a prestigious organization in the healthcare sector, representing approximately 20,000 hospitals across India. Its goal is to unify healthcare providers to work collaboratively with the government and society to enhance the well-being of the common man and build a healthier India. To streamline this mission, AHPI has empowered teams at the state level, with active chapters in Maharashtra, Karnataka, Tamil Nadu, Gujarat, Delhi NCR, Bihar, Haryana, Chhattisgarh, Jharkhand, Andhra Pradesh, Telangana, Rajasthan, Punjab, Kerala, Uttar Pradesh, Madhya Pradesh, Odisha, West Bengal, The North East, and other regions.



FOREWORD

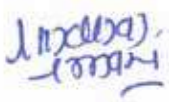
The healthcare environment is one of the most complex and sensitive sectors, where the primary responsibility is not just to provide medical care, but also to ensure a safe and secure environment for patients, staff, and visitors alike. Hospitals, as institutions of healing, must balance these dual priorities to maintain operational efficiency and build trust within the community.

This **Hospital Safety and Security Manual** comes at a critical time when hospitals are faced with unprecedented challenges. With the rise in patient numbers, advancements in technology, and an increasing range of external threats—from natural disasters to security breaches—it is more important than ever to have clear, actionable guidelines in place. A well-prepared healthcare facility is not only equipped to respond to emergencies but is also proactive in mitigating risks, thus ensuring that patient care remains uninterrupted.

This manual offers a comprehensive approach to hospital security, covering crucial aspects such as emergency preparedness, staff training, patient safety protocols, and infrastructure safeguards. It outlines best practices drawn from global standards and real-world case studies, providing hospitals with the tools necessary to create a secure and resilient environment.

As healthcare continues to evolve, so must our approach to safety and security. The strategies outlined in this manual are not static; they are designed to adapt to emerging risks and trends, ensuring that hospitals remain prepared for the future. Association of Healthcare Providers (India) took up the task in preparing this manual, which could be comprehensive in all possible aspects. I commend the members of task force, led by Col (Dr) Sunil Rao (Retd.) for their thorough research and dedication to this vital cause.

This manual is an indispensable resource for all healthcare professionals, administrators, and security personnel who are committed to upholding the highest standards of safety in hospital environments.



Dr. Girdhar J Gyani
Director General
Association of Healthcare Providers (India)



COMPOSITION OF THE TASK FORCE FOR DEVELOPING

'HOSPITAL SAFETY AND SECURITY MANUAL'

Convener: Col (Dr) Sunil Rao, Group CEO, Sahyadri Group of Hospitals Pune

Co-Conveners:

1. Dr Dipak Mitra, Owner Sun Hospital Cuttack
2. Ms Gracy Mathai, CEO Baby Memorial Hospital, Calicut

Security Expert: Mr Barkat Mujawar; Director Vigilance & Security Dr DY Patil University, Pune

Hospital Management Representatives:

1. Dr Sanjay Pathare, Shree Multi-Specialty Hospital Pune,
2. Col (Dr) Bharat Singh, Chief of Medical Services, Sahyadri Hospital Pune

Legal Advisor: Mr Sanyam Khetarpal; practicing advocate in Supreme Court of India

IT Specialist: Mr Saji Mathew; Baby Memorial Hospital Calicut

HR Representative: Mr Umesh Gupta, HR Head MAX Group of Hospitals

Nursing Representatives:

1. Ms Latha Venkatesan, Principal College of Nursing AIIMS New Delhi
2. Ms Roopa Rawat Singhvi, Regional Nursing Lead (SEAR) WHO Collaborating Centre, AIIMS New Delhi
3. Ms Jeena Jose, Nursing Superintendent, Holy Family Hospital Delhi



1 INTRODUCTION

1.1 Purpose

A huge swathe of individuals are required to visit hospital, whether they are their patients, staff, visitors and other service providers, it is important for all hospital facilities to have comprehensive security standards in the form of manual and SoPs to protect hospital environment and hospital staff.

In similar context, Constitution of India provides detailed provisions for safe and healthy working conditions for every working man and woman in the nation. Government recognizes that safety and health of workers has a positive impact on productivity and economic and social development. Similarly, MoHFW announces series of measures to provide additional security to healthcare employees at workplace.

1.2 Scope

Securing premises and personnel from assault, threat, fire hazard, abduction and cyber-attack by internal and external miscreants

1.3 Objectives

- The primary objectives of the Hospital Safety and Security Manual are as under:-
- To assess the current security environment within the different categories of hospitals
- To develop a comprehensive security manual that includes protocols for emergency situations, access control, incident response, and risk management. This would serve as master manual, based on which hospitals can develop manual specific to their conditions.
- To ensure that the security manual is aligned with national and international (for hospitals catering to medical tourism) healthcare security standards

1.4 Definition

Hospital Safety and Security is an essential and inescapable service, especially in a public institution thousands of people visit daily. It is challenging to anticipate the intentions of antisocial elements and to screen visitors without offending them. Additionally, visitors, who may be under stress due to their loved one's illness, are more likely to misunderstand and become upset.

Hospital Safety and Security is defined as "The condition that guarantees that the workers, patients, visitors, infrastructure and equipment within a health care center, are free of risk or danger of accidents".

In general Hospital Safety and Security primarily involves:-

1. Security and safety of the healthcare staff (doctors, nurses, paramedical staff, and housekeeping staff) and workplace violence prevention.
2. Security and safety of patient and their belongings.
3. Security of building.
4. Security of stores and equipment.
5. Security of the public visiting hospital
6. Regulation of traffic to patient care areas, restricted staff-only areas, and public areas.
7. Fire prevention and firefighting.
8. Security from cyber-attack.

2 SECURITY POLICIES

2.1 General Security Policy

Hospital Safety and Security is an essential and inescapable service, especially in a public and private institution, thousands of people visit daily. It is challenging to anticipate occurrence of incidence, the intentions of antisocial elements and to screen visitors. Additionally, the other reasons include, the hospitals are highly prone to various kinds of hazards due to a whole lot of electrical equipment, a laboratory full of chemicals, a huge network of electrical connections, and equipment like CT scans/MRIs working at high tensions.

The prime objective of Hospital Safety and Security for institutions is to ensure that hospital can remain functional and continue providing the necessary health care services during and immediately after the security breach/hazard with more and more emphasis on prevention in breach/hazard.

In general security policy, of hospital must have “security committee”. The committee shall comprise of the following members:-

1. Institutional/Hospital Head
2. Medical superintendent
3. Head laboratory services
4. Head nursing department
5. Security officer
6. Fire safety officer
7. Head biomedical department
8. Head pharmacy services
9. Head IT
10. Head engineering department
11. Head legal department
12. Head quality department
13. Head recruitment/human resource department

The security committee shall conduct Hazard Identification and Risk Analysis (HIRA) and accordingly committee shall develop general security policy considering following elements:-

2.1.1 Purpose: To ensure a safe and secure environment for patients, visitors, staff, and hospital property, this policy outlines the security protocols and responsibilities within the hospital premises.

2.1.2 Scope: This policy applies to all employees, contractors, patients, visitors, and any other individuals on hospital premises.

2.1.2 Policy statement:

1. Access Control and Entry/Exit Systems: Hospital shall implement strict access control measures especially at entrance of OPD, Casualty/Emergency department, billing department, Intensive care area (PICU, NICU), Female in-patient area and mortuary services.
2. Security Personnel: Trained and vigilant security personnel shall be present round the clock in the premises with identified uniform, monitor surveillance systems, and respond to security incidents.
3. Surveillance and Monitoring: Installation of surveillance cameras strategically throughout the hospital premises for monitoring and periodic audit of footage to identify any security breaches shall be incorporated in general policies.
4. Emergency Preparedness and Response: Establish quick response teams (QRTs) for handling emergencies, including bomb threats, fires, and natural disasters. QRTs must be well trained and well worse with various security codes (Code violet, code black, code yellow etc.)
5. Patient and Staff Safety: Laid down policies shall be in place to protect patients and staff from potential threats, including violence, harassment, or abuse. This includes enforcing zero-tolerance policies against violence and ensuring a safe work environment.
6. Protection of High-Value Assets: Identify critical assets within the hospital, such as expensive medical equipment, pharmaceuticals, and patient records and additional security measures for these assets, including restricted access and regular audits must be in place.
7. Language Barriers and Communication: Hospitals often serve diverse populations. Address language barriers by providing multilingual signage and training staff in effective communication. Clear communication during emergencies is essential and key to prevent further harm.
8. Visitor Registration and Identification: All visitors should register upon entry. Provide them with identification badges/pass
9. Human Resources and Training: All stakeholders including contractors, vendors and visitors must comply with this security policy and any additional departmental procedures. Initial briefing with key points on their conduct shall be done at entrance of hospital.
10. Collaboration with Law Enforcement and Regulatory Authorities: Hospital Safety and Security in-charge shall communicate with local law enforcement agencies regularly.
11. Cyber security: Awareness about theft and protection of electronic devices and equipment shall be reviewed periodically.
12. Incident Reporting: Incidence reporting channel shall be displayed and standardized incident report shall be maintained, and investigations will be conducted to prevent future occurrences.

2.2 Employee Security Policy

2.2.1 Purpose:

To establish clear guidelines for hospital staff to ensure the safety and security of patients, visitors, hospital assets, and themselves. This policy aims to prevent security breaches, maintain a secure work environment, and respond effectively to any security incidents.

2.2.2 Scope:

This policy applies to all employees, including full-time, part-time, contractual, and temporary staff, across all departments within the hospital.

2.2.3 Policy Statement:

Hospital staff must adhere to security protocols designed to protect patients, co-workers, and hospital property. All employees are responsible for understanding and following these guidelines, reporting any security concerns, and participating in regular training.

Employee Responsibilities

1. **Identification and Access Control:**
    - **ID Badges:** All employees must always wear their hospital-issued identification badges while on hospital premises. Badges must be visibly displayed above the waist.
    - **Access Permissions:** Employees will be granted access only to areas relevant to their job duties. Any attempt to access unauthorized areas is strictly prohibited.
    - **Lost or Stolen ID:** Report lost or stolen ID badges immediately to the security department to prevent unauthorized access.
2. **Personal Conduct and Security Awareness:**
    - **Suspicious Activity:** Report any suspicious individuals, unattended packages, or unusual activities to Hospital Safety and Security immediately.
    - **Visitor Management:** Verify the identity of all visitors and ensure they are escorted by authorized personnel when in restricted areas.
    - **Professional Conduct:** Avoid engaging in confrontational behavior. Report any threats, verbal abuse, or aggressive actions by patients, visitors, or colleagues to the security department.
3. **Cyber security:** Use of Electronic Devices: Access to hospital information systems must be through authorized devices only. Personal devices should not be used to access sensitive data unless explicitly approved.
    - **Data Protection:** Do not share login credentials, and always log out of systems when not in use. Report any suspected data breaches or cyber security incidents immediately.
    - **Email Security:** Exercise caution when opening emails from unknown sources. Avoid clicking on suspicious links or downloading unverified attachments.

4. **Workplace Safety and Violence Prevention:**
   - **Zero Tolerance for Violence:** The hospital has a zero-tolerance policy for any form of workplace violence, including physical assault, threats, harassment, or bullying. Employees must report any such incidents promptly.
   - **Self-Defense Measures:** Employees should avoid physical confrontations. In case of an imminent threat, use panic buttons or other alarm systems provided by the hospital.
   - **De-escalation Techniques:** Staff will be trained in de-escalation techniques to manage aggressive patients or visitors safely.
5. **Handling Sensitive Information:**
   - **Patient Privacy:** Employees must comply with the hospital's policies on patient confidentiality and data protection as per the Health Insurance Portability and Accountability Act (HIPAA) and other relevant regulations. Refer Image 1
   - **Information Sharing:** Patient information should only be shared with authorized personnel and only when necessary for patient care. Avoid discussing patient details in public areas.



Figure 1

6. **Personal Belongings and Valuables:**
   - **Securing Personal Items:** Employees should secure personal belongings in lockers or designated storage areas provided by the hospital. The hospital is not liable for lost or stolen personal items.
   - **Hospital Property:** Hospital assets, such as medical equipment and electronic devices, must be used responsibly. Report any damage or loss immediately.
7. **Emergency Preparedness:**
   - **Emergency Response Training:** Employees must participate in mandatory training sessions on emergency response protocols, including fire drills, evacuation procedures, and lockdowns.
   - **Communication during Emergencies:** Follow the established chain of command and use designated communication channels during emergencies. Avoid spreading unverified information.
   - **Panic Alarms and Buttons:** Familiarize yourself with the location and use of panic alarms and emergency buttons in the workplace.

SPECIALIZED SECURITY CONSIDERATIONS

8. **Handling High-Risk Patients:**
   - **Behavioral Health Patients:** Staff must be trained to handle patients with psychiatric conditions or substance abuse issues who may pose a risk to themselves or others.
   - **VIP and High-Profile Patients:** Follow special protocols for the security and privacy of VIP or high-profile patients. Access to these patients must be strictly controlled and documented.
9. **Security of Hazardous Materials:**
   - **Controlled Substances:** Employees handling controlled substances must comply with all regulations regarding storage, documentation, and disposal to prevent theft or misuse.
   - **Biohazard Materials:** Follow strict protocols for the handling, storage, and disposal of biohazard materials to prevent contamination or accidental exposure.
10. **Response to External Threats:**
    - **Terrorist Threats:** In case of a bomb threat or suspected terrorist activity, employees must follow the hospital's emergency procedures for evacuation, lockdown, or shelter- in-place.
    - **Natural Disasters:** Staff must be prepared to respond to natural disasters such as earthquakes, floods, or fires, and follow the hospital's disaster management plan.

COMPLIANCE AND ENFORCEMENT

11. **Monitoring and Surveillance:** The hospital will monitor compliance with security policies through surveillance systems, periodic audits, and random checks. Employees found in violation of the security policy may be subject to disciplinary action, including termination of employment.
12. **Training and Awareness:** All employees must attend regular security training sessions and complete mandatory e-learning modules. The hospital will conduct periodic security drills and scenario-based training to enhance preparedness for various security threats.
13. **Reporting and Feedback:** Employees are encouraged to report any security concerns or suggestions to their supervisors or the security department. Anonymity will be respected for those who wish to report concerns confidentially.
14. **Policy Review:** This policy will be reviewed annually or as needed to ensure it remains relevant and compliant with current laws, regulations, and best practices.
15. **Acknowledgment:** All employees are required to acknowledge that they have read, understood, and will comply with this policy. A signed copy of the acknowledgment will be kept in the employee's personnel file.

2.3 Visitor Security Policy

2.3.1 Purpose: To establish guidelines for managing visitor access and behavior within the hospital premises to ensure the safety and security of patients, staff, and hospital property.

2.3.2 Scope: This policy applies to all visitors, including family members, friends, vendors, contractors, and any other individuals who enter the hospital premises.

2.3.3 Policy Statement: The hospital is committed to maintaining a secure environment by controlling visitor access, monitoring visitor activities, and ensuring compliance with all Hospital Safety and Security protocols. Visitors must respect the rules and regulations outlined in this policy to maintain a safe environment.

VISITOR ACCESS CONTROL

1. **Identification and Registration:**
   - **Visitor Registration:** All visitors must register at the main entrance or designated reception area. Registration includes providing valid identification, stating the purpose of the visit, and signing a visitor log.
   - **Visitor Badges:** Visitors will be issued a visitor badge, which must be visibly always worn while on hospital premises. The badge must be returned upon leaving the hospital.
   - **Photo ID Verification:** Photo identification (e.g., Aadhaar card, driver's license, and passport) must be presented at the time of registration. Security personnel may deny entry to visitors who fail to provide valid ID.



Figure 2

2. **Access Permissions:**
   - **Visiting Hours:** Visitors are only allowed during designated visiting hours. Exceptions may be made for critical care or end-of-life situations, with the approval of the hospital administration.
   - **Restricted Areas:** Visitors are restricted from entering certain areas, such as operating rooms, intensive care units (ICUs), staff-only zones, and data centers, unless explicitly authorized by hospital staff.
   - **Accompanied Visits:** Visitors must be accompanied by authorized personnel when accessing sensitive or restricted areas.
3. **Special Circumstances for Visitor Access:**
   - **Children:** Children under the age of 12 are generally not permitted to visit patient areas unless approved by the attending physician or nurse in charge.

- **VIP and High-Profile Visitors:** Special arrangements will be made for VIP or high-profile visitors to ensure their privacy and security. All staff will be notified in advance to prepare for such visits.

VISITOR CONDUCT AND BEHAVIOR

4. **Code of Conduct:**
   - **Respectful Behavior:** Visitors must behave respectfully toward patients, staff, and other visitors. Disruptive behavior, such as shouting, abusive language, or physical altercations, is strictly prohibited.
   - **Prohibited Items:** Weapons, alcohol, illegal drugs, flammable materials, and any other dangerous items are prohibited on hospital premises. Security personnel may conduct searches to enforce this rule.
   - **Electronic Devices:** The use of mobile phones, cameras, and recording devices is restricted in certain areas to protect patient privacy. Visitors must comply with hospital rules regarding the use of electronic devices.
5. **Compliance with Health and Safety Protocols:**
   - **Infection Control:** Visitors must adhere to infection control protocols, such as wearing masks, using hand sanitizers, and following quarantine guidelines, especially in areas with immunocompromised patients.
   - **Personal Protective Equipment (PPE):** Visitors may be required to wear PPE (e.g., masks, gloves, gowns) in certain areas, especially when visiting patients with contagious conditions.
   - **Smoking:** Smoking is prohibited throughout the hospital premises, including outdoor areas, unless a designated smoking area is provided.

SPECIALIZED VISITOR CATEGORIES

6. **Vendor and Contractor Security:**
   - **Vendor Registration:** All vendors and contractors must register at the reception or designated entry point. A background check may be required before granting access.
   - **Supervised Access:** Vendors and contractors will be supervised by authorized hospital personnel at all times. They must adhere to hospital rules and avoid accessing unauthorized areas.
7. **Media Personnel:**
   - **Pre-Approval Required:** Media personnel must obtain prior approval from the hospital administration before entering the premises. They must be always accompanied by a hospital representative.
   - **Photography and Filming:** Photography, video-graphy, or recording within the hospital is strictly prohibited unless explicitly authorized by the hospital administration.

EMERGENCY SITUATIONS

8. **Emergency Protocols for Visitors:**
    - **Emergency Evacuation:** In case of an emergency (fire, natural disaster, security threat), visitors must follow the instructions of hospital staff and security personnel. They should proceed to designated evacuation points and not attempt to re-enter the building until cleared by authorities.
    - **Lockdown Procedures:** During a lockdown, visitors must remain in their current location or follow the directions given by hospital staff or security personnel.
    - **First Aid:** Visitors requiring first aid or emergency medical care while on the premises will be assisted by hospital staff and taken to the nearest emergency department.

ENFORCEMENT AND COMPLIANCE

9. **Monitoring and Surveillance:**
    - **CCTV Monitoring:** The hospital premises are monitored by CCTV cameras for security purposes. Visitor activities are always subject to surveillance. Refer Image 3.
    - **Security Personnel:** Security personnel will conduct regular patrols and checks to ensure visitors comply with all security protocols.



Figure 3

10. **Violation of Security Policies:**
    - **Removal from Premises:** Visitors who violate Hospital Safety and Security policies may be asked to leave the premises immediately. Repeated violations may result in a permanent ban from the hospital.
    - **Legal Action:** In cases of serious misconduct, illegal activities, or threats to safety, the hospital reserves the right to involve law enforcement authorities and take legal action.

VISITOR COMMUNICATION AND FEEDBACK

11. **Information and Signage:**
    - **Clear Signage:** Information regarding visitor policies, visiting hours, and restricted areas will be clearly displayed throughout the hospital. Refer Image 3
    - **Communication Channels:** Visitors can provide feedback or report security concerns through suggestion boxes, online forms, or directly to the hospital's security department.

12. **Regular Policy Review:**
    - **Periodic Review:** This policy will be reviewed annually or as needed to ensure it remains effective and up to date with current security needs and regulations.
    - Policy Updates: Any changes to the visitor security policy will be communicated through hospital signage, staff briefings, and the hospital's official website.
13. **Acknowledgment:**
    - **Visitor Agreement:** By entering the hospital premises, visitors agree to comply with the security policies outlined herein. A copy of this policy will be made available upon request.



Figure 4

2.4 Contractor Security Policy

2.4.1 Purpose: The Contractor Security Policy aims to safeguard the organization's assets, data, and personnel by defining security requirements for contractors, subcontractors, and temporary workers. This policy ensures that all contractors comply with the organization's security standards, minimizing risks associated with unauthorized access, data breaches, and other security incidents.

2.4.2 Scope: This policy applies to all contractors, subcontractors, and temporary workers who access the organization's facilities, systems, networks, or data, either remotely or on-site. It covers all types of information, including proprietary, confidential, and sensitive data.

2.4.3 Policy Overview:

1. **Access Control:**
    - Contractors must undergo identity verification before access to any facility or system.
    - Access to the organization's physical locations and information systems must be based on the principle of least privilege and granted only for the duration of the contracted work.

- All access rights must be reviewed periodically (e.g., monthly or quarterly) to ensure they remain appropriate for the contractor's role.
- Contractors must use organization-approved authentication methods (e.g., multi-factor authentication) for access to any systems.
- A detailed access log must be maintained, documenting all contractor entries and exits, including time, date, and areas accessed.

2. **Data Protection:**
   - Contractors are prohibited from sharing or disclosing any organization data to unauthorized personnel.
   - All data accessed by contractors must be treated as confidential unless explicitly marked otherwise.
   - Contractors must use organization-provided secure communication channels (e.g., encrypted email, VPNs) to access and transmit data.
   - Storage of sensitive data on non-organization devices or external storage media is strictly prohibited.
   - Contractors must immediately report any data breaches, unauthorized access, or loss of data to the designated security officer.
3. **Physical Security:**
   - Contractors must always wear a visible identification badge while on the organization's premises.
   - Contractors are only permitted in areas specified in their contract or as required for their job function.
   - All contractor equipment, such as laptops and USB drives, must be inspected and approved by the organization's security team before being allowed on-site.
   - Contractors are prohibited from taking photographs, videos, or other recordings within the organization's facilities unless expressly authorized.
   - Any suspicious behavior or unauthorized individuals must be reported immediately to the security team.
4. **Cyber security:**
   - Contractors must adhere to the organization's cyber security policies, including software usage, network access, and password management.
   - Contractors must use organization-approved antivirus and endpoint protection software on any device used to access organization systems.
   - Remote access to the organization's network must be made through a secure, organization-approved VPN.
   - Contractors are prohibited from installing, modifying, or deleting any software or data without explicit authorization.
   - Any security vulnerabilities or incidents identified by contractors must be reported immediately to the cyber security team.

5. **Incident Management:**
   - Contractors must follow the organization's incident management procedures in the event of a security incident, breach, or suspected breach.
   - All incidents must be reported to the designated point of contact within the organization without delay.
   - Contractors are required to participate in any investigation or audit related to a security incident involving their actions or systems.
   - Contractors must comply with any instructions or corrective actions issued by the organization's security team following an incident.
6. **Compliance and Audits:**
   - Contractors must adhere to all relevant laws, regulations, and standards (e.g., GDPR, CCPA, HIPAA) that pertain to their work.
   - The organization reserves the right to audit contractor compliance with this policy at any time, with or without notice.
   - Contractors must provide evidence of compliance, such as security certifications, audit reports, or documented procedures, upon request.
   - Non-compliance with this policy may result in termination of the contract and legal action.
7. Training and Awareness:
   - Contractors must complete mandatory security awareness training provided by the organization before beginning any work.
   - Additional training may be required for specific tasks or roles, such as handling sensitive data or accessing critical systems.
   - Contractors are responsible for staying informed about the organization's security policies and any changes to them.
8. **Termination of Access:**
   - All contractors' access to the organization's facilities, systems, and data must be terminated immediately upon completion of the contract, or if the contract is terminated for any reason.
   - Contractors must return all organization-owned property, including ID badges, keys, laptops, and documents, upon termination of access.
   - All contractor credentials, including user accounts and passwords, must be deactivated immediately upon termination of access.
9. **Responsibilities:**
   - **Contractors:** Must comply with all aspects of this policy and report any security incidents or concerns to the organization's security team.
   - **Contractor Managers:** Must ensure that contractors understand and adhere to this policy, conduct regular reviews of contractor access, and report any issues to the security team.

- **Security Team:** Responsible for providing training, monitoring compliance, responding to incidents, and updating this policy as needed.

10. **Enforcement:** Violations of this policy may result in disciplinary action, up to and including termination of the contract, civil or criminal penalties, or both, depending on the nature and severity of the violation.
11. **Review and Updates:** This policy will be reviewed annually, or as required due to changes in laws, regulations, or organizational requirements.

2.5 Emergency Security Policy

2.5.1 Purpose: To establish protocols for the prevention, management, and response to various emergency situations that may arise within the hospital premises, ensuring the safety and security of patients, staff, visitors, and hospital property.

2.5.2 Scope: This policy applies to all hospital personnel, including full-time and part-time employees, contractors, volunteers, and visitors. It covers all emergency situations, including but not limited to fire, natural disasters, internal and external threats, mass casualty incidents, and hazardous material spills.

2.5.3 Policy Statement: The hospital is committed to ensuring a secure and safe environment by preparing for, responding to, and managing emergencies effectively. All employees and personnel must understand their roles and responsibilities during emergencies and follow the established protocols to mitigate risks and minimize harm.

1. Types of Emergencies Covered

- Fire and Smoke Emergencies
- Natural Disaster (eg. Earthquakes, floods, cyclones
- Medical Emergencies (e.g., mass casualty incidents, pandemics)
- Security Threats (e.g., bomb threats, active shooter situations, terrorist attacks)
- Fire and Smoke E Technological Failures (e.g., power outages, equipment failures)
- Hazardous Material Spills (e.g., chemical, biological, radiological, nuclear materials)
- Child abduction
- Violent/assault Incidents (e.g., workplace violence, patient or visitor aggression)

2. Emergency Preparedness and Planning:

a. **Emergency Response Team (ERT):**

- **Formation of ERT:** An Emergency Response Team (ERT) will be formed comprising hospital management, security personnel, medical staff, and trained volunteers. The ERT will be responsible for coordinating emergency preparedness and response activities.
- **Roles and Responsibilities:** The ERT members will have designated roles such as Incident Commander, Medical Coordinator, Security Officer, Communications Officer, and Logistics Coordinator to ensure efficient management of emergencies.

b. **Emergency Protocols and Plans:**

- **Emergency Response Plans:** The hospital will develop specific response plans for each type of emergency, including detailed procedures for evacuation, lockdown, shelter-in-place, and communication.
- **Evacuation Plans:** Evacuation plans must include clearly marked routes, designated assembly points, and provisions for assisting patients with limited mobility.
- **Lockdown Procedures:** Lockdown procedures must be established to secure the hospital in case of internal or external threats, with protocols for sealing entry/exit points and managing access.
- **Shelter-in-Place Protocols:** Shelter-in-place plans must be in place for scenarios such as severe weather or chemical exposure, detailing how and where to seek safety within the facility.

c. **Emergency Supplies and Equipment:**

- **Emergency Kits:** The hospital will maintain emergency kits containing first aid supplies, personal protective equipment (PPE), flashlights, batteries, emergency contact lists, and communication devices.
- **Backup Systems:** The hospital will ensure backup systems, such as generators for power supply and backup communication systems, are functional and regularly maintained.
- **Fire Safety Equipment:** Fire extinguishers, alarms, sprinklers, and other fire safety equipment must be readily available and inspected regularly.

d. **Staff Training and Drills:**

- Regular Training: All hospital staff must undergo regular training on emergency procedures, including fire drills, lockdown exercises, de-escalation techniques, and first aid.
- Scenario-Based Drills: Conduct scenario-based drills to simulate various emergencies, ensuring all personnel are familiar with their roles and responsibilities.
- Emergency Communication: Training on the use of emergency communication devices, such as intercom systems, two-way radios, and mass notification systems, must be provided.

3. Emergency Communication Protocols:

a. **Communication during Emergencies:**

- **Primary Communication Channel:** Use the hospital's intercom system or public address (PA) system for immediate communication during emergencies.
- **Backup Communication Systems:** Maintain backup communication systems, such as two-way radios, satellite phones, and email alerts, to ensure reliable communication in case of primary system failure.
- **Incident Notification:** The ERT must be promptly notified of any emergency via established channels (e.g., hotline, emergency pager, or designated contact number).

b. **Communication with External Agencies:**

- **Coordination with Local Authorities:** Establish communication protocols with local police, fire services, and emergency medical services (EMS) to facilitate a coordinated response.
- **Media Handling:** Designate a Public Information Officer (PIO) responsible for handling media inquiries and providing accurate, timely information to the public while maintaining patient confidentiality.

4. Emergency Procedures by Scenario:

a. Fire and Smoke Emergencies:

- **Immediate Actions:** Activate the fire alarm, notify the ERT, and begin evacuation procedures following the designated routes.
- **Fire Extinguishers:** Trained personnel should use fire extinguishers to control small fires if it is safe to do so. Do not use elevators during a fire.
- **Evacuation of Critical Patients:** Patients in critical care must be evacuated using appropriate equipment (e.g., stretchers, wheelchairs) under the supervision of medical staff.

b. **Natural Disasters:**

- **Earthquakes:** During an earthquake, staff and patients should "Drop, Cover, and Hold On" until shaking stops. Evacuation should only be initiated when it is safe to do so.
- **Floods and Cyclones:** Move to higher ground or safe zones within the hospital. Secure all equipment, documents, and hazardous materials.
- **Post-Disaster Actions:** Conduct a headcount, assess damages, and provide immediate medical assistance to injured individuals.

c. **Medical Emergencies (Mass Casualty and Pandemics):**

- **Mass Casualty Incidents:** Activate the hospital's mass casualty plan, including triage areas, mobilizing additional medical staff, and ensuring adequate medical supplies.
- **Pandemics and Infectious Disease Outbreaks:** Follow protocols for infection control, including isolation areas, use of PPE, and adherence to guidelines from health authorities (e.g., WHO, Ministry of Health and Family Welfare).

d. Security Threats (Bomb Threats, Active Shooter, Terrorist Attacks):

- **Bomb Threat:** Evacuate the area and notify the local police. Do not touch or move suspicious objects. Follow bomb threat checklists and search procedures.
- **Active Shooter:** Implement the "Run, Hide, Fight" protocol: Run if safe, hide in a secure location, or fight only as a last resort.
- **Terrorist Attacks:** Initiate lockdown or evacuation procedures based on the nature of the threat. Cooperate fully with law enforcement and follow their guidance.

e. **Technological Failures:**

- Power Outages: Activate backup generators and emergency lighting. Ensure critical medical equipment is powered and functioning.
- IT System Failures: Follow protocols for manual documentation and communication. Notify the IT department to initiate recovery procedures.

f. **Hazardous Material Spills:**

- **Chemical Spills:** Evacuate the affected area and notify the ERT. Use appropriate PPE and containment measures to prevent further exposure.
- **Biological and Radiological Spills:** Isolate the area and follow decontamination procedures as outlined in the hospital's hazardous materials plan. Alert specialized response teams.

g. **Violent Incidents:**

- **Workplace Violence:** Utilize de-escalation techniques to manage aggressive behavior. If violence escalates, use panic alarms or call security.
- **Patient or Visitor Aggression:** Follow protocols for restraining or removing aggressive individuals, prioritizing the safety of patients and staff.

5. Post-Emergency Actions:

a. **Incident Reporting and Investigation:**

- **Documentation:** All emergencies must be documented in detail, including actions taken, personnel involved, and outcomes. Use incident reporting forms for standardized documentation.
- **Investigation:** Conduct a thorough investigation of the incident to identify causes, assess response effectiveness, and recommend improvements.

b. **Debriefing and Psychological Support:**

- **Debriefing Sessions:** Conduct debriefing sessions with all involved personnel to review the response, identify lessons learned, and provide feedback.
- **Psychological Support:** Provide access to counseling and psychological support for staff, patients, and visitors affected by the emergency.

6. Compliance and Review:

a. **Policy Compliance:**

- **Monitoring:** Regular audits and drills will be conducted to ensure compliance with emergency protocols.

- **Disciplinary Actions:** Non-compliance with emergency procedures may result in disciplinary action, including suspension or termination.

b. **Policy Review:**

- **Regular Updates:** This policy will be reviewed annually or after any major incident to ensure it remains current and effective.
- **Stakeholder Feedback:** Incorporate feedback from staff, patients, and local authorities in policy revisions to enhance emergency preparedness.

7. Acknowledgment:

- **Staff Acknowledgment:** All staff members are required to read, understand, and acknowledge this Emergency Security Policy. A signed acknowledgment will be maintained in the personnel file.

2.6 Patient Privacy and Confidentiality

2.6.1 Purpose: To protect the privacy and confidentiality of all patient information, ensuring compliance with applicable laws, regulations, and ethical standards. This policy outlines the measures to prevent unauthorized access, use, disclosure, or destruction of patient data.

2.6.2. Scope: This policy applies to all hospital personnel, including full-time and part-time employees, contractors, volunteers, and any other individuals who have access to patient information. It covers all forms of patient data, including electronic, paper-based, verbal, and any other format.

2.6.3 Policy Statement: The hospital is committed to safeguarding patient privacy and confidentiality by implementing strict security measures and protocols. All personnel must understand their responsibilities to protect patient information and always comply with this policy.

1. Definitions:

a. **Key Terms:**

- **Patient Information:** Any information that relates to the past, present, or future physical or mental health or condition of a patient, including demographic data, medical history, test results, and treatment details.
- **Protected Health Information (PHI):** Patient information that is created, received, stored, or transmitted by the hospital, which must be protected under applicable privacy laws.
- **Unauthorized Access:** Any access to patient information by individuals who do not have permission or a legitimate need to know.

2. Data Privacy and Confidentiality Principles:

a. **Principles of Patient Data Protection:**

- **Data Minimization:** Only collect and retain the minimum amount of patient information necessary for the intended purpose.
- **Access Control:** Limit access to patient information to authorized personnel only, based on their job responsibilities.

- **Integrity and Confidentiality:** Ensure the accuracy, completeness, and confidentiality of patient information throughout its lifecycle.
- **Accountability:** Hold all personnel accountable for adhering to this policy and reporting any breaches or violations.

3. Security Measures for Patient Privacy:

a. **Physical Security:**

- **Restricted Access:** Secure areas where patient information is stored (e.g., medical records rooms, IT data centers) with access control systems, such as keycards or biometric scanners. Only authorized personnel should have access.
- **Locked Storage:** Store paper-based patient records in locked cabinets or rooms with restricted access. Records should not be left unattended in public or unsecured areas.
- **Secure Disposal:** Dispose of physical patient records securely through shredding or incineration to prevent unauthorized access or retrieval.

b. **Electronic Data Security:**

- **Data Encryption:** Use encryptions for all electronic patient information stored on hospital systems, devices, or transmitted over networks. Encryption must meet industry standards (e.g., AES-256).
- **Access Controls:** Implement role-based access controls (RBAC) and multi-factor authentication (MFA) to prevent unauthorized access to electronic health records (EHR) and other patient data systems.
- **Regular Audits:** Conduct regular audits and monitoring of access logs to detect unauthorized access or suspicious activity. Immediate action must be taken in case of any breaches or anomalies.

c. **Network and IT Security:**

- **Firewalls and Intrusion Detection Systems (IDS):** Deploy firewalls and IDS to protect hospital networks from cyber-attacks and unauthorized access.
- **Patch Management:** Regularly update and patch all software, operating systems, and applications to protect against known vulnerabilities.
- **Data Backup and Recovery:** Implement regular data backup procedures and maintain an offsite backup to ensure data integrity and recovery in case of a data breach or loss.

4. Employee Responsibilities:

a. **Confidentiality Agreements:**

- **Signed Agreements:** All employees, contractors, and volunteers must sign a confidentiality agreement upon joining the hospital, acknowledging their understanding and commitment to protect patient privacy.
- **Regular Training:** Provide mandatory training on patient privacy and data security protocols, including recognizing phishing attacks, secure handling of patient data, and reporting potential breaches.

b. **Secure Handling of Patient Information:**

- **Verbal Communication:** Discuss patient information only in private settings and avoid public or common areas where unauthorized individuals might overhear.
- **Email and Messaging:** Use secure, encrypted email or messaging platforms approved by the hospital when communicating patient information. Do not use personal email accounts or unauthorized messaging apps.
- **Paper-Based Information:** Minimize the use of paper-based records. When used, ensure they are handled securely and not left unattended in public areas.

5. Patient Rights and Consent:

a. **Patient Rights to Privacy:**

- **Right to Information:** Patients have the right to know how their information is being collected, used, and shared. Provide patients with a clear and concise privacy notice at the time of admission.
- **Consent for Use:** Obtain explicit consent from patients before using their data for purposes beyond their direct care (e.g., research, marketing). Document all consent forms securely.
- **Right to Access and Amend:** Patients have the right to access their own medical records and request amendments if they believe the information is inaccurate or incomplete.

b. Third-Party Access and Data Sharing:

- **Controlled Data Sharing:** Limit sharing of patient information with third parties (e.g., insurance companies, external labs) to only what is necessary and in compliance with patient consent and legal requirements.
- **Business Associate Agreements:** Ensure that all third parties with access to patient data sign business associate agreements (BAAs) to comply with hospital privacy and confidentiality standards.

6. Critical and Niche Security Issues:

a. **Data Breaches and Cyber security Threats:**

- **Incident Response Plan:** Develop and maintain a data breach response plan, including procedures for immediate containment, investigation, notification, and remediation.
- **Phishing and Social Engineering:** Implement regular training sessions on phishing and social engineering attacks and establish clear procedures for reporting suspicious emails or behavior.
- **Dark Web Monitoring:** Consider using dark web monitoring services to detect and mitigate potential breaches where patient information is sold or traded online.

b. **Insider Threats:**

- Behavioral Monitoring: Implement monitoring tools to detect unusual behavior by employees with access to sensitive data, such as unauthorized downloads or accessing records not related to their duties.

- Background Checks: Conduct thorough background checks for employees, contractors, and volunteers with access to patient information to identify any potential risks.

c. **Privacy Concerns with Modern Technologies:**

- **Internet of Things (IoT) Devices:** Secure all IoT devices (e.g., smart monitors, connected medical devices) with strong passwords, regular software updates, and network segmentation to prevent unauthorized access.
- **Telehealth Services:** Ensure all telehealth platforms used for remote consultations are secure, compliant with privacy laws, and equipped with end-to-end encryption.

d. **Handling Genetic and Biometric Data:**

- **Sensitive Data Protections:** Treat genetic and biometric data with heightened sensitivity due to its unique nature and potential for misuse. Ensure this data is encrypted, anonymized where possible, and only accessible to authorized personnel.
- **Research Protocols:** Implement strict protocols for using patient data in research, ensuring that ethical standards, anonymization, and patient consent requirements are met.

e. **Social Media and Public Communication:**

- **Social Media Use:** Prohibit the sharing of any patient information on personal or professional social media platforms. Staff must be trained on the consequences of such actions.
- **Public Statements:** Only designated hospital spokespersons may make public statements involving patient information, and they must adhere to all privacy regulations.

7. Reporting and Incident Management:

a. **Reporting Privacy Breaches:**

- **Immediate Reporting:** All personnel must report any suspected or confirmed breaches of patient privacy to the Data Protection Officer (DPO) or designated authority immediately.
- **Whistleblower Protection:** The hospital will protect whistleblowers who report breaches or unethical practices in good faith from any form of retaliation.

b. **Incident Investigation and Mitigation:**

- **Breach Investigation:** A designated team, including IT, legal, and risk management, will investigate all reported breaches to determine the cause, impact, and necessary corrective actions.
- **Notification to Affected Parties:** In the event of a data breach involving patient information, the hospital will notify affected patients promptly and provide guidance on steps they can take to protect themselves.

8. Compliance and Review:

a. **Compliance Monitoring:**

- **Regular Audits:** Conduct regular audits of patient privacy and confidentiality practices to ensure compliance with this policy and relevant laws and regulations.
- **Disciplinary Actions:** Non-compliance with this policy may result in disciplinary action, including termination and legal consequences.

b. **Policy Review:**

- **Annual Review:** This policy will be reviewed annually or in response to significant changes in legal requirements, technology, or hospital practices to ensure its continued effectiveness.
- **Stakeholder Input:** Incorporate feedback from patients, staff, and regulatory bodies into the policy review process.

c. **Acknowledgment:**

- **Staff Acknowledgment:** All staff members are required to read, understand, and acknowledge this Security Policy for Patient Privacy and Confidentiality. A signed acknowledgment will be maintained in their personnel file.

3 SECURITY PERSONNEL

3.1 Roles and Responsibilities

Every hospital staff and other stakeholders have a responsibility for Hospital Safety and Security and should report any concerns to their immediate hierarchy or superior, in the first instance. However, specific role and responsibility related to key appointments are as under:-

Serial Number	Key appointment	Role and responsibility
	Security committee	• Develop, propose, review and revision of security policies and procedures for hospital. • Review all incidences to evaluate and implement necessary additional security practices to prevent future incidence. • Review all reported incidences and make recommendation to hospital head regarding financial and non-financial implications. • Conduct and present security audit periodically to hospital head and implement suggestions. • Keep records of meeting with information in the channel of hierarchy.
	Security personnel	• Being a visible authoritarian figure capable of deterrence. • Guarding high-footfall areas and monitoring all visitors • Checking the identification or passes of visitors or issuing them passes • Taking charge of metal detector and bag-checking security procedures • Preventing access to and photo in in hospital premises. • Performing routine inspections in the areas they are guarding. • Monitoring activities on security camera video monitors. • Staying alert and observant, and reporting suspicious activities to security officer. • Recognizing potential threats and taking steps to mitigate them. • Participating in rescue operations with firefighters and police. • Detecting criminal or dangerous and detaining possible suspects in hospital. • Announce security code immediately if unable to handle situation. • Advising people about necessary safety precautions.

	Security Officer	• Coordination with external security agencies. • Establishing and monitoring of security control centre of hospital • Conduct security audit and present findings to security committee. • Project requirement to respective department related to security. • Ensure night patrolling and securing the area. • Control on surveillance equipments, monitoring and analyzing CCTV camera footage on daily basis. • Specific guarding and monitoring of vulnerable area of hospital. • Immediate response to security code, disorderly conduct, disruptive persons and arranging manpower, material and machine with the help of respective staff. • Keeping an incident report record. • Ensure checking (entrance and exit) and escorting visitors around the hospital premises. • Ensure secure all entry (doors, windows) and exits depending on shift. Investigate any security related incidence and present to security committee with recommendations.
	Institutional/ Hospital Head	• Execution of policies and procedure. • Execution of recommendation of security committee inconsonance with defined policy and procedure for hospital. • Provide financial and non-financial support for 100% secure hospital.
	Medical Superintendent	• Administrative control on security of hospital. • Oversee the functioning of security committee. • Implement recommendation of security committee, policies and procedure. • Conduct surprise round and security code announcement to check preparedness of hospital staff and department. • Ensure that every hospital staff, visitors, patients and contractor is trained and follows all applicable policy and procedure related to Hospital Safety and Security. • Ensure contingency plan ready for executive emergencies especially for bedridden patient (In case of fire, mob attack, abduction, critical equipment failure and sexual assault)

	Head nursing department	• Formulation and review policy and procedure on security of nursing staff including night shift of female staff. • Ensure the comfortable hospital facilities for nursing staff as far as practicable. • Ensure self-defense training of nursing staff. • Ensure on-ground feedback from patients with the help of subordinates about secure hospital environment. • Ensure professional etiquette of nursing staff. • Conduct surprise round in female hostel/ward to find out any gap in security.
	Fire safety officer	• Developing and implementing Fire Safety Policies. • Conducting inspections and risk assessments regularly. • Ensure the hospital fire safety complies with local, state, and national fire safety rule & regulations with regular & immediate collaboration. • Conduct fire safety training sessions for hospital staff to educate them about fire hazards, proper use of firefighting equipment, evacuation procedures, signage and other relevant safety protocols. • Investigating the cause of the fire, analyze the circumstances leading up to the fire, identify any lapses in fire safety protocols, and make recommendations for security committee to prevent future incidents. • Oversee regularly the maintenance and testing of fire detection & suppression systems. • Coordinate in case of fire hazard, leading up evacuation procedures, and ensure that everyone safely exits the hospital building. • Conduct fire safety mock drill and raise awareness among hospital staff about the importance of fire safety and secure escape of patient. • Monitor the procurement, installation, and maintenance of fire safety equipment at and inside the hospital premises. Even ensure that all the systems are installed correctly, regularly inspected, and promptly repaired if any issues arise. • Maintain detailed records related to fire safety inspections, training sessions, equipment maintenance, and emergency response drills.

	Head biomedical department	• Planning, projecting, Procuring, Installation, calibration, AMC, CMC, preventive and corrective maintenance of medical devices and equipment. • Monitoring of assets tracking system for medical devices and equipment in various areas of hospitals. • Conduct investigation of incidence happed due to equipment failure and make recommendations to security committee. • Monitoring and back up of critical care equipments. • Update software as per policy and purchase order. • Daily monitoring with check list of critical equipment's at critical area of the hospitals like critical/intensive care areas including blood bank. • Maintain complaint log register and ensure timely resolution of problems. • Conduct regular training about functioning and safety of medical devices and equipment for end user.
	Head pharmacy services	• Plan, organize, and direct pharmacy services and operations to ensure safe, accurate, and efficient dispensing of medications. • Ensure secure storage of medicine to prevent theft and security of pharmacy assets. • Ensure that controlled substances are dispensed in compliance with the law and that inventory control and record keeping requirements are met. • Implement and modify pharmacy policies and procedures according to established pharmaceutical principles and regulatory requirements. • Ensure an efficient training program is in place for the hospital staff.
	Head IT	• Provide direction, consulting, approve, administration and monitor major projects, IT budgets, priorities, standards, procedures, and overall IT performance. • Regular Periodic review and evaluate current systems and applications for external threat (Cyber-security). • Ensure provisioning of UHID and security of data as per privacy and data policy inconsonance with state and national guidelines. • Collaborate with the different departments of hospital for training on cyber threat and its prevention. • Scheduling upgrades and security backups of hardware and software systems. • Provide network accounts and passwords as required. • Secure disposal of IT equipment and hardware as per e-waste management rule.

	Head engineering department	• Planning, projecting, Procuring, Installation, calibration, AMC, CMC, preventive and corrective maintenance of non-medical devices and equipment (Lifts, Gen set, UPS, HVAC, AC Plant, Hospital Lighting etc) • Ensure uninterrupted electrical supply to medical equipment with 24x7 power back for critical equipment. • Conduct electrical hygiene audit for hospital and make recommendations for security committee. • Daily monitoring with check list of critical equipment required for critical area of the hospitals. • Maintain complaint log register and ensure timely resolution of problems. • Conduct regular training about functioning and equipment for end user.
	Head legal department	• Providing legal guidance on a wide range of legal matters such as contracts, regulatory compliance, litigation, employment law, intellectual property. • Identifying and mitigating legal risks. • Conduct training for hospital staff about general awareness in legal/statutory requirement. • Drafting, negotiating and vetting contracts, legal documents and agreements. • Reporting incidence to local/state/national authority as and when required.
	Head quality department	• Developing, implementing, and monitoring key performance indicator for security & safety to ensure standards, regulations, and best practices in hospital operations. • Identifying, assessing, and mitigating potential risks to patient and hospital staff, this involves implementing robust incident reporting and root cause analysis processes. • Collecting, analyzing, and interpreting data to identify areas for improvement, track progress, and provide comprehensive reports to security committee.

	Head human resources	• Recruitment of appropriate security staff. • Ensure smooth induction and periodic training of hospital staff about security and safety. • Appreciation and award for best practices in actual and during mock drill. Similarly, ensure Grievance Redressal Committee (GRC) functioning and timely redressal of complaint. • Receive, analyze and monitoring the complaint against work place harassment. • Implements wellness initiatives, counseling services, and other programs to support the physical and mental well-being of hospital staff.
	All hospital staff	• Comply with all security policy, procedures and instructions that are applicable to his/her own actions and conduct • Refrain from any unsafe act that might endanger him/herself or fellow staff • Meticulous use of all security devices and personal protective equipment provided for his/her protection • Report all hazards, incidents, and near-miss occurrences to their immediate supervisor or security committee • Proactively participate in security training and surveys as requested and provide input into how to improve security • Do not use defective tools or machinery. Report them to superior immediately • Familiarize with all signs, posters, warnings, firefighting equipment, security code and exits throughout hospital area • Be alert and vigilant for hospital visitors, patient and unidentified article.

3.2 Training and Certification

Hospital safety and security becomes an important responsibility and hospital liability to create safe and secure environment because of the numerous hazards & safety risks present in a hospital. As the public becomes more knowledgeable and aware of such risks, they demand such safety and security provision in the hospitals.

Regular training in the form of education, mock drill play important role in prevention of harm due to security lapses. Here, training of hospital staff means:-

- Have the knowledge and skills needed to work safely and preventing harm and hazards that could place themselves or others at risk.
- Demonstrate awareness and understanding of security concern and how to identify, report, and control them.
- Receive specialized training when their work involves unique hazards.

Similarly, training may be evaluated based on following key performance indicator:-

- Man hour of training in the unit
- Man days of training conducted
- Man days of training attended
- Improvement in skill to handle specific scenario

Structured training program may be developed by hospital as per risk assessment and it can be implemented in following stepwise manner:-

1 **Awareness training:** Provide hospital staff a basic understanding of the training structure, plans, and procedures. This knowledge ensures that everyone can fully participate in training. There shall be mandatory training for all hospital staff, contractor during induction as well as periodic on following topic:-

- Various security code (Code yellow, black, violet etc)
- Fire safety
- Patient fall prevention
- Hospital signages (Exit route and hospital blue print)
- Cyber security
- Assets tracking
- Electrical hygiene
- Incidence reporting
- Legal compliances and local law enforcing agencies
- Self defense
- Anti-harassment policy of hospital

2. **Specialised training:** Additional training may be needed to ensure that hospital staff can incorporate responsibilities for secure hospital environment into their daily routines and activities like Mob handling, Communication skills, handling of unidentifiable articles, security check at entrance, exit and sensitive areas (Casualty department, NICU, PICU, Mortuary, Billing department etc).

Now a day various public and private institutes conducting the certification and diploma courses related to security and that can be considered during hiring process for qualification criteria:-

- International College for Security Studies- Certification in cyber and physical security
- Indian Institute of skill development – Diploma in security officer
- National Institute of Electronics & Information Technology- Cyber security certification

3.3 Communication Protocols

Communication protocol is important for healthcare staff and all who interact with healthcare system. Hospitals must continue to communicate to their internal and external stakeholders in view of timely recognition of threat to hospital environment. Five basic elements must be considered while communicating with internal and external stakeholders. Refer Image 5

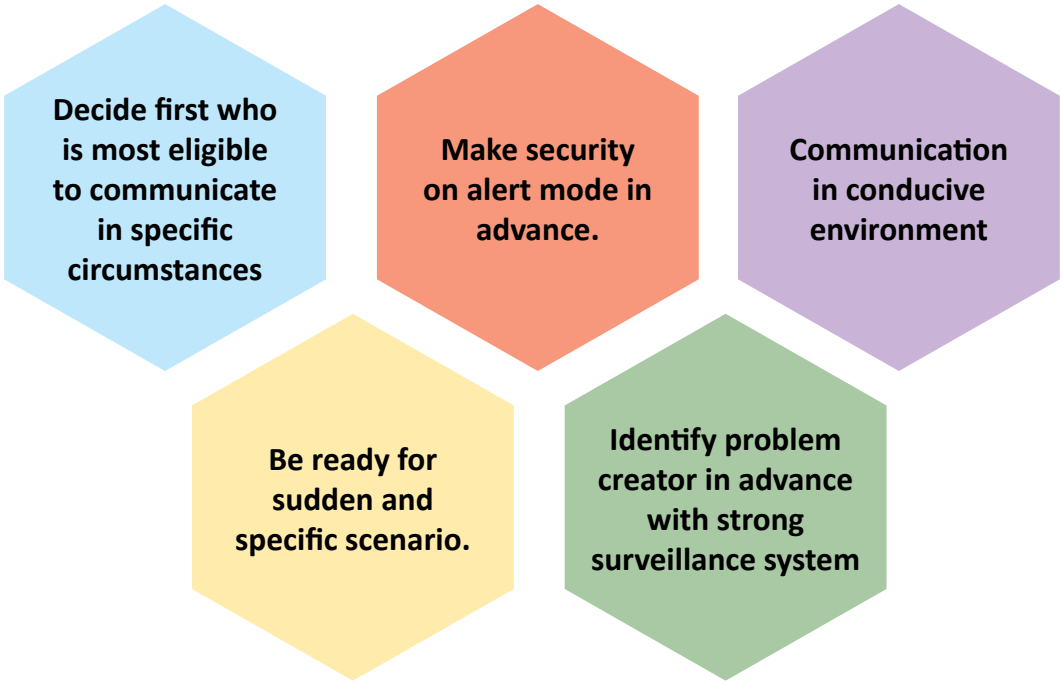


Figure 5

1 **Protocol for communicating with patients, family members or other visitors:** Following points as a protocol shall be considered while communicating with patients, family members or other visitors:-

- Prior knowledge about issue.
- Informal action if issue is grave.
- Sit down, make them comfortable, lean forward and make eye contact.
- Find out what the patient/understands.
- Be empathetic (Acknowledge a patient's emotions explicitly).
- Ask before you tell.
- Note down if so much in conversation.
- Provide information slowly and deliberately.
- Use short statements and explanations (Avoid long monologues).
- Watch the body language and facial expression.
- Be prepared for a reaction. When delivering bad news, it is important for the hospital staff to be prepared, recognize the response by the patient, allow sufficient time for a display of emotions, and listen quietly and attentively.
- Make positive and partnership statement.

2 **Protocol for communicating mass/crowd:** Those managing healthcare facilities should focus their efforts on following as a protocol:-

- Good communicator- Source trust and credibility are key principles of a successful communication. In order to ensure a proper level of preparedness and a prompt response to crowd, communicators have to be recognized as "trusted sources" from

the attendees. Trust could depend on direct experience as well as historical, socio-cultural, or legal reasons.

- Message delivery- Crowd has specific expectations on the information they need. They ask for detailed information. On the contrary, often communicators are able to provide only the main information, because the time is missing.
- Communication through external agency- hospital shall have a list of emergency contacts immediately available including:
  - Police
  - Community leaders
  - Religious leaders
  - Media
- **Information exchange-** Quick information exchange between hospital administration, department heads and other hospital staff.
- **Information and Communication Technology (ICT)** use like Walkie-Talkie and public announcement system, if required.

3.4 Uniform and Identification

A security uniform is a standardized set of clothing worn by security personnel while on duty. Its primary purpose is to distinguish security guards from the patients, visitors, relatives, medical & paramedical staff, ensuring they are easily recognizable in various area of hospital. This visibility is crucial for maintaining order and providing reassurance to those in the vicinity.

Uniforms play a critical role in the security of hospital by serving multiple functions:-

- **Visibility:** Highly visible uniforms deter potential wrongdoers by signaling the presence of security.
- **Authority:** Uniforms confer a sense of authority and professionalism, making it easier for security personnel to perform their duties.
- **Psychological Impact:** Uniform's formal appearance can influence public perception and behavior, promoting a sense of safety and secure environment.
- **Team Unity:** Uniforms foster a sense of belonging and unity among security staff, which can be crucial for coordinated actions in case of threat.

3.5 Performance Evaluation

Security of hospital is very sensitive and serious issue; because even minor oversights can have significant consequences, which is why security personnel performance evaluations are essential for minimizing these risks. Regular evaluations act as a proactive measure, identifying knowledge gaps or areas where procedures might not be fully understood or practiced.

Following are the key reasons why employee performance evaluation is important:

- **Feedback and Improvement:** It fosters a culture of continuous learning and development, encouraging security personnel to seek opportunities for self-improvement.

- **Accountability:** Accountability encourages security personnel to take initiative, be proactive, and demonstrate greater commitment to their roles.
- **Addressing Weaknesses:** Addressing weaknesses proactively with hospital support can mitigate performance issues and improve overall security team performance.
- **Enhanced Communication:** Improved communication can lead to stronger trust, expectation and rapport between security personnel and security officer.

A Sample format for performance evaluation of security personnel given below and can be modified as per hospital requirement for continuing improvement:-

PERFORMANCE EVALUATION			
Name	**Staff ID**	**Department**	**Period covering**
Evaluator name -1 (Immediate superior)	Evaluator name-2 (Security officer)	Evaluation date	Next Evaluation
RATING SCALE			
Excellent-5, Good-4, Average-3, Poor-2, Very poor-1			
Criteria	**Description**	**Rating (1-5) by Immediate superior**	**Rating (1-5) by Security officer**
Reliability	Consistency in attendance and punctuality.		
Professional Development	Engagement in training and self-improvement.		
Teamwork	Ability to work well with others.		
Incident Response	Efficiency and effectiveness in handling incidents.		
Adherence to Protocols	Compliance with Hospital Safety and Security procedures.		
Demeanor	Clean and professional uniform with proper identification displayed. Behavior and communication with other.		

POST EVALUATION FEEDBACK TO SECURITY STAFF	
Immediate superior	
Security officer	

SIGNATURE AND DATE		
Security staff	Immediate superior	Security officer

4 ACCESS CONTROL

4.1 General Access Control

4.1.1 Introduction: Access control in a large hospital setting is critical for ensuring the safety of patients, staff, visitors, and sensitive assets. This manual provides guidelines and Standard Operating Procedures (SOPs) for implementing and maintaining effective access control systems in hospitals. It covers physical and digital access control, visitor management, and the necessary protocols for security and safety.

4.1.2 Objective of access control:

- Ensure the safety of patients, staff, and visitors.
- Protect sensitive areas such as operating rooms, drug storage, and medical records.
- Prevent unauthorized access to restricted areas.
- Provide a secure environment for hospital operations.
- Comply with local regulations and privacy laws.

4.1.2 Physical Access Control

- **Keycard and Badge Systems:** Staff members are issued ID cards or badges with embedded RFID or magnetic strips to access authorized areas.
- **Biometric Systems:** Fingerprint, facial recognition, or iris scan systems may be used for higher security areas such as pharmacies, ICUs, and data centers.
- **Turnstiles and Gates:** These restrict entry to authorized personnel in high-security areas or staff-only zones.
- **Lock and Key Systems:** Mechanical locks are still used for certain non-critical areas but are being phased out in favor of electronic systems.

4.1.3 Digital Access Control

- **Login Credentials:** Digital access controls such as passwords and PINs are required to access electronic health records (EHRs) and other hospital management systems.
- **Multi-Factor Authentication (MFA):** Ensures secure access to sensitive digital systems by requiring two or more forms of authentication (e.g., a password and a fingerprint).
- **Role-Based Access Control (RBAC):** Access to digital systems is assigned based on job roles (e.g., doctors, nurses, or administrative personnel).

4.2 Staff Access Control

- **General Access:** Staff members have access to common hospital areas such as staff rooms, offices, and patient care units based on their job role.
- **Restricted Access:** Critical areas such as operating rooms, ICUs, maternity wards, and pharmacies are accessible only to authorized personnel (e.g., surgeons, nurses, pharmacists).
- **High-Security Access:** Areas containing medical records, IT data centers, and drug storage facilities require biometric access and are limited to key personnel.

4.3 Visitor Access Control

- **Public Areas:** Visitors are granted access to waiting areas, general lobbies, and cafeterias.
- **Patient Rooms:** Access to patient rooms is managed based on visitation hours and hospital policies.
- **Escorted Access:** Visitors and attendants must be escorted by hospital staff when accessing semi-restricted zones like post-surgery recovery areas.
- **Temporary Access:** Contractors and vendors are granted temporary access to relevant areas, with credentials revoked after work completion.
- **Supervised Access:** In high-security areas, contractors must be escorted by Hospital Safety and Security or staff.

4.4 Access to Sensitive Areas (e.g., IT rooms, ICU, Pediatrics)

- **Escort Requirements:** Visitors should be escorted by staff when accessing sensitive or restricted areas.
- **Surveillance Integration:** Access control points should be monitored via CCTV cameras to ensure that access is being used properly and to identify potential breaches.
- **Automated Alerts:** The system should generate alerts when unauthorized access attempts occur, allowing security personnel to respond immediately.
- **Direct access:** Only to be given to key appointments.
- **Access Reviews:** Access permissions should be reviewed regularly to ensure they are up to date, particularly when staff roles change.

4.5 ID Badges and Access Cards

- **Registration and ID Verification:** Visitors and attendants must be registered at the entrance with valid IDs. Temporary visitor badges with specific access zones should be issued. Similarly, key hospital staff only to provide access card not for visitors.
- **Temporary Badges:** Visitors should be issued temporary badges with access to specific areas. These badges must be visibly worn at all times.
- **Badge Return:** Badges must be returned upon exit and verified by security personnel to ensure they have not been used improperly.

4.6 Handling Lost or Stolen Access Credentials

- **Redundant Storage:** Implement redundant storage solutions to ensure data is not lost due to hardware failures.
- **Off-Site Backups:** Regularly back up critical footage to off-site or cloud storage to protect against on-site disasters. Ensure redundancy by storing backups in a separate location or cloud.
- **Encryption and Security:** All surveillance data, both stored and transmitted, should be encrypted to protect against unauthorized access.

5 SURVEILLANCE SYSTEM

5.1 CCTV and Monitoring Systems

5.1.1 Introduction: The implementation of CCTV and monitoring systems in a large hospital is essential for maintaining the safety and security of patients, staff, and visitors. This manual outlines the guidelines and Standard Operating Procedures (SOPs) necessary for the effective deployment and management of these systems.

5.1.2 Primary Objectives:

- Enhance the security of patients, staff, and visitors.
- Monitor sensitive and restricted areas to prevent unauthorized access.
- Deter criminal activities such as theft, vandalism, or assault.
- Assist in incident investigations by providing video evidence.
- Ensure compliance with safety protocols and regulations.

5.2 Placement of Cameras

Placement of Cameras		
Critical Areas	Emergency Rooms and ICUs	Continuous monitoring is crucial for patient safety and incident response
	Pharmacy and Drug Storage	Surveillance prevents unauthorized access to medications and controlled substances
	Operating Rooms and Post-Operative Areas	Cameras should be placed outside these areas to monitor access without compromising patient privacy
	Data Centers and Server Rooms	Surveillance is necessary to protect sensitive patient data and IT infrastructure.
Public Areas	Main Entrances and Exits	Cameras should cover all entry and exit points to monitor the flow of people.
	Waiting Rooms and Lobbies	Ensures that these areas remain safe and orderly for patients and visitors.
	Parking Lots and Garages	Surveillance deters theft, vandalism, and other criminal activities.

Placement of Cameras		
Restricted Areas	Administrative Offices	Monitored to prevent unauthorized access to sensitive information.
	Staff Rooms and Break Areas	Ensures the safety and security of hospital staff during off-duty hours.
Privacy-Sensitive Areas	Patient Rooms	Cameras should not be placed inside patient rooms to protect privacy, but corridors outside these rooms should be monitored.
	Restrooms and Changing Areas	These areas must not have surveillance to respect privacy, but adjacent hallways can be monitored.

Additional Camera Placement Considerations

1. **Dynamic Monitoring in Emergency Situations:** Install mobile or portable CCTV units that can be deployed in temporary or high-risk areas during emergencies (e.g., pandemics, mass casualty events).
2. **Blind Spot Minimization:** Periodically review camera placements to identify and eliminate blind spots, especially in critical areas like hallways and stairwells.

Special Considerations for Sensitive Areas

1. **Access Restrictions for Psychiatric Units:** Implement specialized access control measures in psychiatric units, such as heightened access restrictions, to protect both patients and staff.
2. **Secure Data Center Access:** Use advanced access control measures, such as mantraps or dual authentication, to secure entry points to data centers, ensuring the protection of sensitive data.

5.3 Surveillance Monitoring and Review

Real-Time Monitoring

1. **Continuous Surveillance:** Security personnel should monitor live feeds continuously, especially in critical areas.
2. **Automated Alerts:** The system should be configured to send alerts in case of unusual activity (e.g., forced entry, prolonged loitering).
3. **Incident Logging:** Any incidents observed should be logged with time stamps for later review.

Incident Response

1. **Immediate Action:** Security personnel must respond promptly to incidents detected via CCTV (e.g., deploying security to the location).
2. **Incident Reporting:** All incidents must be reported to the appropriate hospital authorities and documented for future reference.

Remote Monitoring

1. Access Control: Only authorized personnel should have access to remote monitoring feeds.
2. Secure Connections: Remote access should be secured with encryption to prevent unauthorized viewing or data breaches.

Incident Review Protocols

1. Standard Operating Procedure (SOP): When an incident occurs, footage should be reviewed by designated personnel following predefined protocols.
2. Chain of Custody: Any footage used for legal or disciplinary reasons must follow a strict chain of custody to ensure it is admissible in investigations.
3. Post-Incident Reviews: After a security incident, conduct a full review of the footage and assess the efficiency of the response. Regular audits should be conducted to ensure the system is functioning properly.

Advanced Surveillance Technologies

1. Facial Recognition Technology: Consider implementing facial recognition for monitoring high-risk areas (e.g., ICUs, OT, drug storage). Ensure compliance with privacy laws and obtain necessary consents.
2. AI-Powered Analytics: Use AI-based video analytics for automated detection of unusual activities, such as loitering in restricted areas or suspicious behavior. This can improve response times and reduce manual monitoring efforts.

Enhanced Access Control Protocols

1. **Dual Authentication for High-Security Areas:** Introduce dual authentication (e.g., card swipe and biometric scan) for access to critical areas like operating theaters, ICUs, and data centers.
2. **Temporary Access Codes for Contractors:** Generate unique, time-bound access codes for contractors and vendors to ensure they have limited access during specified periods. Codes should automatically expire after the allotted time.

Visitor and Attendant Management Enhancements

1. **Digital Visitor Passes:** Use digital visitor passes with QR codes to simplify visitor management. Passes can be scanned at entry points to verify access permissions and time limits.
2. **Pre-Registration of Visitors:** Enable pre-registration for visitors, allowing them to fill out required information online, reducing congestion at entry points, and ensuring smoother access control.

5.4 Recording and Storage of Surveillance Data

Data Retention Policies

1. **Retention Period:** Surveillance data should be retained for a specified period (e.g., 30-90 days) based on hospital policy and legal requirements.

2. Extended Storage: Data related to incidents should be archived and stored for longer periods as required by investigations or legal processes.

Backup and Redundancy

1. Redundant Storage: Implement redundant storage solutions to ensure data is not lost due to hardware failures.
2. Off-Site Backups: Regularly back up critical footage to off-site or cloud storage to protect against on-site disasters.

Data Deletion Protocols

1. Automatic Deletion: Implement automatic deletion protocols to remove data after the retention period, ensuring compliance with data protection regulations.
2. Secure Deletion: Ensure that deleted data cannot be recovered, particularly when footage contains sensitive information.

5.5 Data Privacy and Usage

Access Control for CCTV Footage

1. Restricted Access: Access to recorded footage should be limited to authorized personnel, such as security managers, hospital administrators, and legal authorities.
2. Audit Trails: Maintain an audit trail of who accessed surveillance footage, when, and for what purpose.

Legal Compliance

1. Compliance with Local Laws: Ensure that the use of CCTV systems complies with local regulations and privacy laws, including notification and consent requirements.
2. Patient and Staff Rights: Patients, staff, and visitors should be informed about the use of CCTV in the hospital and their rights concerning recorded footage.

Privacy and Ethical Considerations

1. Patient Consent Management: Develop a consent management system to handle situations where patient consent is required for certain types of surveillance (e.g., use of cameras in specific treatment areas).
2. Privacy Impact Assessments (PIAs): Conduct regular PIAs to evaluate the impact of surveillance activities on patient privacy and implement mitigative measures as needed.

Usage Guidelines

1. Prohibited Uses: CCTV footage must not be used for purposes unrelated to safety and security, such as monitoring staff productivity.
2. Ethical Considerations: Footage should be used responsibly, with respect for the privacy and dignity of individuals.

6 INCIDENT RESPONSE

6.1 Incident Reporting Procedures

6.1.1 Incident Identification and Reporting: The first step in managing incidents is identifying and reporting them. Incidents may involve patient safety, medication errors, equipment failures, or environmental hazards.

a. **Types of Incidents:** These include adverse events, near-misses, and no-harm incidents. For example, a patient receiving the wrong dose of medication or a surgical instrument left inside a patient.

b. Reporting Process: Hospitals encourage staff to report incidents promptly and transparently, often through online systems or designated incident reporting forms. Some hospitals have anonymous reporting options to encourage openness.

6.1.2 Incident Categorization: After being reported, incidents are categorized based on their severity, impact, and type. This helps prioritize and determine the level of investigation required.

Categories of Incidents:

c. **Clinical Incidents:** Related to patient care (e.g., medication errors, surgical complications).

d. **Non-Clinical Incidents:** Related to hospital operations (e.g., equipment failure, power outages).

e. **Workplace Incidents:** Related to staff safety (e.g., injuries, staff abuse, or burnout).

Severity Levels: Minor, moderate, severe, or catastrophic.

6.1.3. Risk Assessment and Prioritization: Once categorized, each incident undergoes a risk assessment to determine its potential impact on patient safety, staff, or hospital operations.

- **Tools used:** Hospitals often use tools like the Risk Matrix to assess the likelihood and severity of harm.
- **Goal:** To prioritize high-risk incidents for immediate action while managing lower-risk events in an appropriate timeframe.

6.1.4. Investigation and Root Cause Analysis (RCA): A formal investigation is conducted to determine the underlying causes of the incident. This often involves a Root Cause Analysis (RCA) to identify systemic issues rather than individual fault. Refer Image 6

Steps in RCA:

a. **Data Collection:** Gathering detailed information about the incident (who, what, when, where, how).

b. **Analysis:** Identifying contributing factors (human errors, environmental conditions, faulty equipment).

c. **Root Cause Identification:** Understanding the deeper systemic or process issues that led to the incident.

d. **Involvement:** A multidisciplinary team, including clinical and non-clinical staff, often leads the investigation to ensure a holistic perspective.

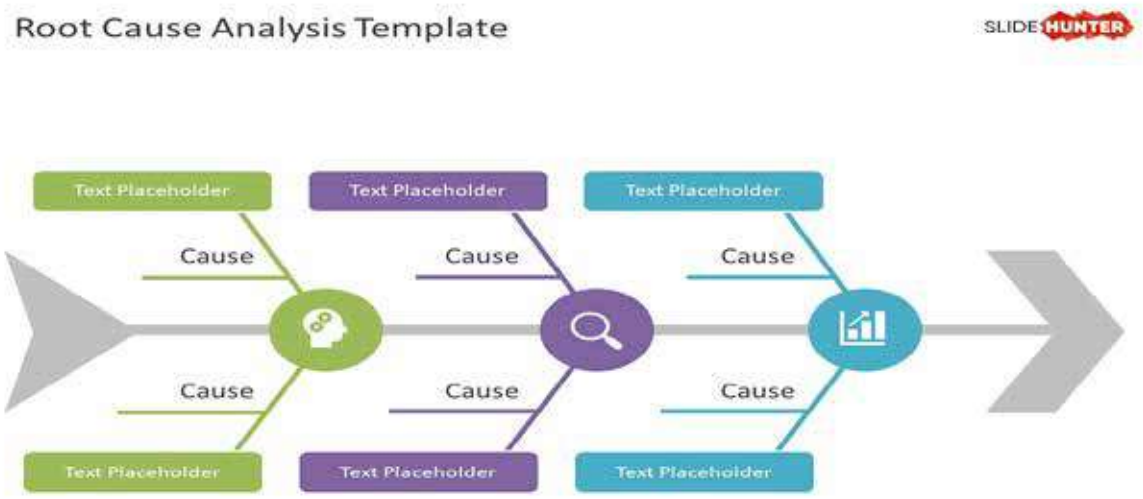


Figure 6

6.1.5. Immediate Response and Containment: Immediate steps are taken to contain the incident and prevent further harm. This may involve stopping a procedure, withdrawing a medication, or isolating equipment.

- **Example:** If a medication error is detected, the hospital would immediately notify the prescribing physician and nurse to assess the patient and take corrective action.
- **Temporary Measures:** Containment measures may be temporary (until a permanent solution is found) or permanent, depending on the investigation's findings.

6.1.6. Corrective and Preventive Actions (CAPA): Based on the RCA, corrective actions are implemented to address the current incident, and preventive actions are designed to avoid recurrence.

a. **Corrective Actions:** Focus on resolving the immediate issue (e.g., staff retraining, adjusting medication protocols).

b. **Preventive Actions:** Aim to address systemic issues, such as implementing new technologies (e.g., barcode scanning for medication administration) or revising policies.

c. **Monitoring Effectiveness:** CAPA actions are regularly reviewed to ensure they are effective in reducing risks.

6.2 Emergency Response Protocols: Proper response and communication protocol of the incident, both internally and externally, is critical to ensure transparency, accountability, and effective management.

6.2.1 Internal Communication: Hospital leadership, staff, and affected departments are informed about the incident and any necessary changes.

6.2.1 External Communication: In severe cases, communication with patients, families, and sometimes the media may be required. Hospitals must also comply with reporting obligations to health authorities.

6.2.3 General protocol:



Figure 7

a. **Conduct a risk assessment:** The first step to ensure effective emergency response protocols is to conduct a risk assessment. A risk assessment helps to prioritize the most urgent and likely risks, and to determine the resources and capabilities needed to address them.

b. **Develop clear roles and responsibilities:** The second step to ensure effective emergency response protocols is to develop clear roles and responsibilities for all the stakeholders involved in the emergency response.

c. **Establish communication and coordination mechanisms:** The third step to ensure effective emergency response protocols is to establish communication and coordination mechanisms among the stakeholders. Communication (formal and informal) and coordination are essential for sharing information, providing guidance, requesting and offering resources, and resolving conflicts and issues.

d. **Provide training and education:** The fourth step to ensure effective emergency response protocols is to provide training and education for all the stakeholders. Training and education are necessary for building the knowledge, skills, and attitudes required for effective emergency response.

e. **Evaluate and improve:** The fifth step to ensure effective emergency response protocols is to evaluate and improve them on a regular basis. Evaluation and improvement are crucial for identifying the strengths and weaknesses of the emergency response protocols, and for making adjustments and enhancements based on the feedback and data collected from the stakeholders.

6.3 Coordination with Local Law Enforcement

6.3.1 Purpose of SOP: This Standard Operating Procedure (SOP) is established to provide comprehensive guidelines that will enable coordination with health facilities and external agencies. The purpose of this SOP is to ensure that there is systematic and effective collaboration in all contacts between the health facility and local law enforcement, emergency services, public health authorities, and social services.

6.3.2 Scope: This SOP will involve all personnel in healthcare facilities, with a wide array of activities involving managerial teams that oversee and implement procedures, clinical teams that are directly involved with patient care and at times need to liaise with the external agencies, and administrative personnel who handle the documentation and communication aspects of coordination. It also covers the scope of both emergency and non-emergency situations so that all staff will be prepared to engage external agencies effectively for various situations.

6.3.3. Roles and Responsibilities: Effective coordination with external agencies is a team effort within healthcare facilities. Each department and staff member plays a critical role in ensuring smooth collaboration, contributing to both the safety of the institution and the quality of patient care.

Note: Detailed elaboration on the subject "Role and Responsibility" & "Coordination with External Agencies" are provided under chapter 3 & 10)

6.4 Incident Documentation and Follow-up: Comprehensive documentation of the incident, investigation, and actions taken is essential for accountability, legal protection, and regulatory compliance.

a. **Documentation Systems:** Most hospitals use electronic systems to record incident reports, investigation findings, and corrective actions.

b. **Regulatory Requirements:** In some cases, incidents must be reported to external bodies, such as health authorities, accreditation agencies

6.5 Post-Incident Review and Improvements

6.5.1 Follow-Up and Monitoring: After corrective actions are taken, the hospital continues to monitor the situation to ensure that the changes are effective and that similar incidents do not occur.

a. **Ongoing Audits:** Periodic reviews, audits, and incident trend analysis help ensure continuous improvement.

b. **Performance Metrics:** Hospitals track key performance indicators (KPIs), such as the number of incidents reported, response time, and the impact of corrective actions.

6.5.2 Learning and Continuous Improvement: Incident management is a key component of a hospital's overall quality improvement and patient safety programs. Hospitals use incident data to improve processes and train staff.

a. Safety Culture: By learning from incidents, hospitals foster a culture of safety where staff feels empowered to report errors and near misses without fear of punishment.

b. Staff Training and Education: Hospitals often implement training programs based on lessons learned from incidents to prevent recurrence.

7 PHYSICAL SECURITY MEASURES

7.1 Perimeter Security

a. Fencing and gated entrances: Forming a strong perimeter requires a thorough strategy. The 5 D's of perimeter security showcases the multiple layers of security needed to protect a site's assets, they also allow for time and the intelligence needed to quickly respond to security threats.
   - Deter
   - Detect
   - Defend
   - Delay
   - Deny

b. **Perimeter intrusion detection system (PIDS):** security systems designed to detect and prevent unauthorized entry into a defined perimeter. These systems can use a variety of technologies such as sensors, cameras, and alarms to detect intrusions and alert security personnel or law enforcement.

The solution comprises of the following components:

- Electrical Smart Power Fence (ESPF)
- CCTV camera including thermal cameras
- UPS power supply
- IT infrastructure (Hardware and Software)

7.2 Security Lighting

7.2.2 Interior security lighting

a. **Entrance and Reception Areas**
   - **Lux Level:** 300-500 lux.
   - **Lighting Type:** Use high-CRI (Color Rendering Index) LED lights to accurately render colors and improve facial recognition by CCTV cameras.
   - **Design Considerations:** Ensure all entry points and reception desks are brightly lit, creating a welcoming yet secure environment. Consider overhead lighting combined with wall-mounted fixtures to eliminate shadows.

b. **Hallways and Corridors**

- **Lux Level:** 150-200 lux.
- **Lighting Type:** Continuous linear LED fixtures or recessed ceiling lights for uniformity. Emergency backup lighting should be installed to ensure consistent illumination during power outages.
- **Design Considerations:** Illuminate all hallways and corridors uniformly. Avoid areas where shadows might form, such as behind doors or in alcoves. Install additional lights at intersections to enhance visibility.

c. **Waiting Areas**

- **Lux Level:** 200-300 lux.
- **Lighting Type:** Combination of ceiling-mounted LEDs and soft, diffused lighting to avoid glare and harsh shadows.
- **Design Considerations:** Provide even, glare-free lighting to support security monitoring and comfort. Lighting should ensure visibility for security staff and CCTV without being overly harsh for waiting individuals.

d. **Stairwells and Elevators**

- **Lux Level:** 200-300 lux.
- **Lighting Type:** Bright LED wall sconces or recessed ceiling lights, with motion sensors in stairwells for energy efficiency.
- **Design Considerations:** Ensure stairwells and elevator lobbies are well-lit to prevent them from becoming hiding spots. Motion-activated lighting can enhance energy savings while ensuring safety.

e. **Patient Rooms**

- **Lux Level:** 100-150 lux (ambient), 300 lux (task lighting near beds).
- **Lighting Type:** Dimmable LED lights with options for patient-controlled lighting, plus night lights that provide low-level illumination without disturbing sleep.
- **Design Considerations:** Ensure patient rooms have controlled lighting to prevent unauthorized access, especially in high-security wards. Emergency alert lights should be bright and attention-grabbing without causing distress to patients.

f. **Staff Areas**

- **Lux Level:** 300-500 lux.
- **Lighting Type:** LED panel lights or downlights to ensure bright, even illumination.
- **Design Considerations:** Staff areas should be well-lit to prevent unauthorized access. Use lighting to support clear visibility of staff ID badges and to create a secure.

g. **Emergency Departments**

- **Lux Level:** 500-750 lux.
- **Lighting Type:** High-output LED lights with dimming capabilities for flexibility during emergencies.
- **Design Considerations:** Maintain high visibility to support rapid response and deter aggressive behavior. Crisis lighting should include the ability to increase brightness or activate strobe effects to alert staff to an ongoing incident.

h. **Pharmacies and High-Security Areas**

- **Lux Level:** 500-750 lux.
- **Lighting Type:** Bright, controlled LED lights with integrated alarm-triggered flashing lights.
- **Design Considerations:** Pharmacies and secure areas should have bright lighting to prevent theft. Integrate lighting with security systems so lights can flash or change color during a security breach.

7.2.3 Exterior Lighting for Crime Prevention

a. Building Perimeter

- **Lux Level:** 100-200 lux.
- **Lighting Type:** High-pressure sodium (HPS) or metal halide floodlights for large areas, with LED spotlights for targeted illumination.
- **Design Considerations:** Ensure continuous lighting around the building's perimeter, particularly at fences, gates, and other access points. Lighting should be consistent to prevent shadows where intruders could hide.

b. **Parking Lots and Garages**

- **Lux Level:** 75-150 lux.
- **Lighting Type:** High-intensity discharge (HID) or LED pole lights with wide distribution patterns.
- **Design Considerations:** Provide bright, even lighting to eliminate dark spots and enhance visibility. Lights should be placed to support CCTV coverage, and motion-activated lights can be used in less frequented areas.

c. **Walkways and Pathways**

- **Lux Level:** 50-100 lux.
- **Lighting Type:** Bollard lights, pathway lights, or in-ground LEDs that provide low-level, focused illumination.
- **Design Considerations:** Pathways should be evenly lit to prevent tripping hazards and ambush opportunities. Use lighting to guide people along secure routes, especially from parking areas to building entrances.

d. **Entrances and Exits**

- **Lux Level:** 300-500 lux.
- **Lighting Type:** LED wall packs or canopy lights that provide bright, directed illumination.
- **Design Considerations:** Entrances and exits should be brightly lit to ensure these critical points are visible and under surveillance. Emergency exit lighting should be clearly marked and illuminated for visibility.

e. **Loading Docks and Service Areas**

- **Lux Level:** 200-300 lux.
- **Lighting Type:** LED floodlights with motion sensors and security-enhanced fixtures that resist tampering.

- **Design Considerations:** Ensure these areas are well-lit to deter unauthorized access and enhance visibility during security patrols. Lighting should be robust and resistant to tampering.

f. **Landscaping and Green Spaces**

- **Lux Level:** 50-100 lux.
- **Lighting Type:** LED landscape lights, in-ground lights, or spotlights that highlight critical areas without creating hiding spots.
- **Design Considerations:** Use lighting to illuminate landscaping, reducing the risk of these areas being used for criminal activity. Ensure that lighting is positioned to avoid obstructions by trees or shrubs.

g. **Signage and Way finding**

- **Lux Level:** 100-150 lux.
- **Lighting Type:** Backlit signs or LED floodlights focused on signage.
- **Design Considerations:** Ensure all directional and wayfinding signage is well-lit to help visitors navigate safely. Emergency alerts or instructions should be visible at night and in low-light conditions.

7.2.4 Special Considerations

a. **Coordination with Security Systems**

- **Integrated Systems:** Lighting should be integrated with CCTV, alarms, and access controls to ensure a cohesive security environment. Lights should be programmed to respond to security breaches, such as flashing or brightening when an alarm is triggered.
- **Remote Monitoring:** Use smart lighting systems that can be monitored and controlled remotely by security personnel. This includes the ability to adjust lighting levels in real-time based on security needs.

b. **Emergency Situations**

- **Emergency Lighting:** Ensure that all critical areas have emergency lighting that activates automatically during power outages or security breaches. This includes exit pathways, stairwells, and assembly points.
- **Visible Alarm Indicators:** Install lighting that visually indicates when an alarm is triggered, such as flashing lights or color changes, to help security personnel respond quickly.

c. **Energy Efficiency**

- **LED Lighting:** Utilize energy-efficient LED lighting that provides bright illumination while minimizing energy consumption. LEDs are particularly suited for 24/7 environments like hospitals due to their long lifespan and low maintenance needs.
- **Sustainable Practices:** Implement sustainable lighting practices, such as using solar-powered lights for exterior pathways or motion-activated lights to reduce energy use when areas are unoccupied.

d. **Regular Maintenance and Inspections**

- **Routine Checks:** Conduct regular maintenance and inspections to ensure all lighting systems are functioning properly. This includes checking for burned-out bulbs, damaged fixtures, and ensuring emergency lighting is operational.
- **Immediate Repairs:** Address any lighting issues, such as malfunctioning fixtures or broken controls, immediately to maintain a secure environment. Regularly update and test the lighting system to ensure it meets the evolving needs of the hospital.

7.3 Alarm Systems

7.3.1 Introduction: A hospital, more than any other institution, is exposed to emergencies and life- threatening situations – from medical emergencies like cardiac arrest, accidents, casualties and disasters to dangers arising from fire and bomb threat. It has to be all the more alert to these situations because nowhere else are such a large number of helpless people concentrated in one place and are so utterly dependent on other people for their safety and health. Build-in safeguards and preparedness are the essence of all safety programmes. The alarm system is one such programme.

7.3.2 Fire alarm: Every hospital must have a fire alarm system, which should be a part of the hospital's electrical system. Wherever possible, it should be designed to transmit an alarm signal directly to the telephone operator so that she can contact the fire department and notify the hospital personnel without any loss of time. The fire alarm system can be automatic or it can be operated manually. Smoke and fire detection devices are installed in the patient rooms and other high-risk areas in the heating and ventilating ducks between the floors. These actuate the fire alarm system. On activation, the system sounds alarms throughout the premises or zones, including distinctive visual and audible alarm signals at the respective nurses' station. To indicate the location of fire, there is an indicator light outside every room. This is activated when there is a fire in the room. In the automatic system, smoke detectors not only activate the fire alarm signals, but also close smoke doors and simultaneously shut off fans in the central air handling system. If the fire alarm system is not automatic, then anyone noticing or hearing the fire signal should immediately inform the telephone operator who, in turn, will call the fire department, and notify the hospital personnel.

7.3.3 Medical Gas Alarm: In the centralized medical gas system, oxygen and nitrogen oxide which are stored in bulk in the manifold room are distributed to other areas of the hospital such as the operating rooms, ICUs and patient rooms through pipelines. Compressed air and vacuum (suction) are supplied through pipes to certain areas. Two kinds of alarm are incorporated into the medical gas system. One monitors the pressure of various gases at different areas of the distribution system. If abnormal pressure is sensed, the system sets off an alarm – the green signal goes off and the red warning signal glows with audible alarm until the line pressure returns to normal. The second alarm is called the remote signal lamp which is generally only visible. The lamp lights up when either of the banks of cylinders becomes empty. The remote signal lamp is only a warning signal. No immediate action is necessary because when one bank is empty, the other takes over and supplies the gas without interruption. The alarm should be located in the medical gas user areas such as the operating rooms and patient floors as well as the main working area where the medical gas system is maintained. However, these areas

especially the maintenance area, may not be manned all the time. Secondary signals should therefore be installed in places like the telephone operator's room, security office and the like where a 24-hour attendance is assured.

7.3.4 Blood Bank Alarm: Most hospitals use specially crafted refrigerators – a cold room or walk-in cooler is ideal- to store whole blood in the blood bank. These refrigerators are set to a particular temperature to maintain blood in good condition and are provided with an alarm. The alarm, which is both audible and visual goes off whenever it senses high temperature or a drop in voltage. If the blood bank or the laboratory of which it is a part is not manned round the clock, the alarm signals should be located both in the blood bank and in a place that has 24-hour attendance.

7.3.5 Narcotics Alarm: Narcotics are stored in locked and be in the cabinets in nurses' stations as well as in the pharmacy. There are restricted drugs, which are constantly stolen by persons addicted to them. Some hospitals install a signal system that illuminates a light bulb that is visible from the nurses' station and the corridors whenever the narcotics cabinet door is opened.

7.3.6 Cold Room and Walk-in Cooler Alarm: Many hospitals have walk-in coolers or cold rooms in their food service department and laboratory. They have been instances of the staff of the food service department getting accidently locked up overnight inside the walk-in coders. There should be an alarm button that can be used in such an emergency with a distinguishable audible and visual alarm indicator in a prominent area where there is a 24-hourpersonnel coverage.

7.3.7 Voltage Fluctuation Alarm: In any hospital where sensitive and expressive equipment worth crores of rupees is used, stabilized voltage is essential. Motors are usually designed to withstand only a 10% fluctuation in voltage supply. Beyond this limit, the motor will get damaged unless it is disconnected. Low voltage poses the biggest threat to electrical system and equipment. Diagnostic equipment often gives erroneous readings in low voltage conditions. There are certain areas and sensitive equipment that do not tolerate excessive low or high voltage. Such areas or equipment may be fitted with a simple voltage-sensitive alarm along with a voltmeter. The alarm can be set at any desired point.

7.3.8 Elevator Alarm: Many hospitals have more than one passenger and bed-cum-passenger elevators, which are in continuous operation. Whenever there is an electric power failure, elevators with their passengers get stranded, often in between floors. In order to rescue the stranded passengers, a panic or emergency push button is provided in each elevator. When it is pressed, a battery-operated alarm installed in the electric room or the security room, which is manned round the clock, is actuated to alert people about the rescue operation. Elevator operators or maintenance crew then manually which down the elevator car from the machine room to the next floor to rescue the stranded passengers. Modern elevators have a leveling feature that automatically taxes the elevator car to the next floor level in case of power failure.

7.3.9 Security Alarm: Certain sensitive areas of the hospital like the cashier's office, the psychiatric ward, bank extension counter and pharmacy which are prone to theft and burglary or where patients suddenly become violent need to summon immediate help from security personnel. Some hospitals provide alarm systems in these areas. The alarm may be of two kinds. One is an automatic alarm like the one used in strong rooms of banks or jewelry shops

which goes off when someone tries to break in. The other is similar to the one used by bank tellers. The device is activated by the employee to summon security or police help.

7.3.10 Patient Emergency Alarm: Various new features are now available that can be incorporated into the conventional nurse call system to meet emergency situations in the patient rooms. If the nurse does not respond to the patient's call immediately, the system makes the light outside the patient's room and on the nurse call panel in the nurse station blink. If there is still no response, the blinking of lights and the beep signals from the bleeper on the panel gradually keep increasing in frequency. An additional feature that can also be fitted into the nurse call system is the panic button in the patient toilet that the patient can activate by suing a pull cord in case of emergency.

7.3.11 Code Blue Alarm: Code blue is a term used in hospitals to announce or signal an emergency of a serious nature such as a cardiac arrest. In some hospitals, in all patient rooms and other strategic location, there are independent buttons – not a part of the nurse call system – named Code Blue which when activated emit distinguishable emergency alarm signals both at nurse's station and at the telephone operator's room. While the nurse attends to the patient instantly, the telephone operator goes on the public address instantly, the telephone operator goes on the public address system announcing Code Blue three times giving the location of the emergency. In such hospitals, there is a written procedure to deal with such situations and pre-appointed Code Blue team which respond to the call instantly. The members of the team are trained to deal with medical emergencies including cardiac arrest.

7.3.12 Panic button

a. **Types of Panic Buttons**

Wearable Panic Buttons

- **Design:** Consider options like lanyards, badges, wristbands, or even smartwatch-style devices. The design should be discreet yet accessible.
- **Features:** Look for devices with features like GPS tracking, two-way communication, and vibration alerts to confirm activation.
- **Durability:** Ensure that wearables are durable, waterproof, and resistant to hospital conditions (e.g., exposure to disinfectants).

Fixed Panic Buttons

- **Placement:** Install these in areas where staff are often stationary, such as nurses' stations, reception desks, and consultation rooms.
- **Ease of Access:** Buttons should be easily accessible but discreetly placed to prevent accidental activations.
- **Multiple Buttons:** Consider installing multiple buttons in larger rooms or areas where staff may be spread out.

Figure 8

b. **Integration**

- **Existing Systems:** Ensure the panic button system can integrate with the hospital's current security infrastructure, including CCTV, access control, and communication systems.
- **Alert Protocols:** Set up the system to trigger alerts in multiple formats (e.g., SMS, email, PA announcements, and security monitoring dashboards).

c. **Emergency Protocols**

- **Response Teams:** Identify and train specific teams responsible for responding to panic button alerts. Define clear roles and responsibilities.
- **Alert Escalation:** Develop a tiered alert system where initial alerts are sent to nearby staff, with escalation to security or management if the situation is not resolved within a set time frame.
- **Communication Channels:** Establish clear communication channels for different types of alerts, such as minor incidents vs. major emergencies.

d. **Regular testing and monitoring**

- **Routine Checks:** Schedule regular system checks, including testing all fixed and wearable panic buttons, network connectivity, and system responsiveness.
- **Drill Schedule:** Implement a regular schedule for drills to ensure that staff remains familiar with the system and response protocols.
- **Update Rollouts:** Plan for regular software and firmware updates to keep the system secure and functional.

7.4 Lockdown Procedures

7.4.1 Lockdown procedures: It is critical component of a healthcare facility's emergency preparedness plan. Lockdowns may be necessary in response to situations such as active shooter incidents, violent intruders, hostage situations, or external threats such as civil disturbances or nearby criminal activity. A well-developed lockdown plan ensures the safety of patients, staff, and visitors by controlling movement, securing areas, and mitigating risks during such emergencies.

Here's a detailed guide to creating and implementing effective emergency lockdown procedures in healthcare facilities:

1. Types of Lockdowns

Types	Definition	Purpose
Full Lockdown	This involves securing the entire hospital or facility. No one is allowed to enter or exit the building. Movement within the hospital is also restricted. Full lockdowns are usually activated in response to immediate internal threats (e.g., active shooter, violent intruder).	To protect staff, patients, and visitors from an immediate threat within or near the hospital.

Types	Definition	Purpose
Partial Lockdown	This involves securing specific areas within the hospital while other parts of the facility continue to function. It is often used when the threat is localized (e.g., a violent patient in one department, or a suspicious person in the vicinity)	To contain the threat to a particular area and prevent it from spreading while ensuring that critical operations in other parts of the facility remain functional.
External Lockdown	In this scenario, the hospital secures all external entry points, preventing anyone from entering or leaving the facility. This is typically used when there is an external threat (e.g., nearby criminal activity or a violent protest).	To protect the hospital from external threats without interrupting normal internal operations.

7.4.2 Key Components of a Lockdown Procedure

a. **Initiating the Lockdown**

- **Threat Assessment:** Hospitals should have a security team responsible for assessing threats and determining whether a lockdown is necessary. This could include monitoring alarms, surveillance cameras, or receiving real-time updates from local law enforcement.
- **Authorized Personnel:** Clearly define who has the authority to initiate a lockdown. This could include Hospital Safety and Security personnel, the hospital administrator, or an emergency response team leader.
- **Activation Mechanism:** Lockdown initiation should be immediate and easy to activate. Facilities may use a combination of:
  - Panic buttons strategically located throughout the hospital.
  - Electronic access control systems to automatically lock doors.
  - Communication systems to notify all staff and patients of the lockdown.

b. **Communication during Lockdown**

- **Lockdown Announcements:** Use the hospital's internal communication system (e.g., PA system, text alerts, intercoms) to announce the lockdown. Messages should be clear, concise, and provide instructions, such as:
  - "The facility is now in lockdown. All staff and visitors, please remain in place. Secure doors and windows, and do not leave your area until further notice."
- **Code Words:** To avoid alarming patients or visitors, many hospitals use code words to announce a lockdown. For example, "Code Silver" for an active shooter situation or "Code Yellow" for a suspicious person.
- **Two-Way Communication:** Ensure that all departments have a way to communicate with security or the incident command team during the lockdown. This could include two-way radios, dedicated phone lines, or secure messaging systems.

c. **Securing the Facility**

- **Locking Doors:** As soon as a lockdown is initiated, all exterior doors should automatically lock, preventing unauthorized entry or exit. Interior doors leading to critical areas (e.g., operating rooms, ICUs) should also be secured.
- **Controlled Access:** For healthcare facilities with electronic access control, automatically lock down high-security areas, such as pharmacies, pediatric wards, or areas with controlled substances.
- **Manual Locking:** In areas without electronic access control, staff should manually lock doors and secure entrances. Ensure that keys or codes for manual locks are easily accessible to authorized personnel.

d. **Patient and Staff Safety during Lockdown**

- **Sheltering in Place:** Staff and patients should remain where they are during the lockdown. Encourage them to secure doors, cover windows, and stay out of sight. Patients who can be moved should be relocated to safer, more secure areas when necessary.
- **Critical Areas:** Some hospital areas, such as the emergency room (ER), operating theaters, and intensive care units (ICU), may not be able to halt operations during a lockdown. Ensure that staff in these areas receive special instructions on how to secure their workspaces while continuing essential patient care.
- **Securing Sensitive Areas:** Areas containing hazardous materials, medications, or sensitive medical equipment should be secured immediately. Lock cabinets, drawers, and rooms to prevent unauthorized access.
- **Assisting Patients and Visitors:** Staff should remain calm and reassure patients and visitors, especially vulnerable populations (e.g., children, the elderly, psychiatric patients). Ensure clear communication and provide instructions to visitors.

7.4.3 Staff Roles and Responsibilities

a. **Security Team**

- **Lockdown Initiation and Monitoring:** The security team is responsible for initiating the lockdown, monitoring the facility via security cameras, and ensuring all access points are secured.
- **Coordination with Law Enforcement:** Work closely with local law enforcement to provide real-time updates on the situation. Provide floor plans, access codes, or other essential information to assist law enforcement when they arrive on-site.
- **Managing Access Points:** During a lockdown, security should prevent unauthorized entry or exit, ensuring the facility remains secure.

b. **Incident Command Team**

- Overall Coordination: This team manages the hospital's response during the lockdown, including communication with staff, coordinating patient safety measures, and liaising with external responders such as law enforcement or emergency medical services.

- Communication Hub: They are responsible for communicating updates to all hospital departments and ensuring that critical areas receive real-time information about the lockdown's status.

c. **Hospital Staff**

- **Patient Safety:** Medical and support staff should focus on securing their immediate areas while ensuring the safety of patients. This may include relocating patients to safer areas, securing medical equipment, and following lockdown protocols.
- **Visitor Management:** Instruct visitors to remain in place during the lockdown and assist them in finding secure locations if they are in public spaces such as waiting rooms or cafeterias.

7.4.4 Releasing the Lockdown

a. **Coordination with Law Enforcement**

- **Approval to Lift Lockdown:** Only lift the lockdown once local law enforcement confirms the threat has been neutralized or controlled. Law enforcement should communicate directly with the incident command team before the lockdown is officially lifted.
- **Secure Areas during Lockdown Release:** After the lockdown, maintain heightened security until the entire facility is deemed safe. Continue monitoring sensitive areas (e.g., pharmacy, ICU) and check for any suspicious activity or damaged equipment.

b. **Post-Lockdown Communication**

- **Lockdown Release Announcement:** Use the hospital's PA system or mass notification system to announce the end of the lockdown, clearly stating: "The lockdown has been lifted. Staff and visitors may now resume normal activities. Thank you for your cooperation."
- **Debriefing with Staff:** After the lockdown, conduct a debriefing session with all hospital staff, especially those directly involved in the emergency response. Discuss what worked well and identify areas for improvement in future lockdown procedures.

7.4.5 Training and Drills for Lockdown Procedures

a. **Staff Training**

- **Annual Lockdown Training:** All hospital staff, including medical personnel, administrative staff, and security teams, should undergo lockdown procedure training at least once a year. This training should include:
  - Recognizing when a lockdown is necessary.
  - Procedures for securing patients and visitors.
  - Communicating during the lockdown.
- **Role-Specific Training:** Tailor training for specific roles, such as security personnel, who need advanced skills in coordinating with law enforcement, or ICU nurses, who must balance patient care with security.

b. **Lockdown Drills**

- **Regular Drills:** Schedule regular lockdown drills (at least annually) to test the hospital's response to a lockdown scenario. Drills should simulate realistic scenarios, such as active shooter incidents, and involve coordination with law enforcement.
- **Post-Drill Evaluation:** After each drill, conduct an evaluation with all departments and external partners (e.g., local law enforcement). Identify any weaknesses or challenges encountered during the drill and update the lockdown procedures accordingly.

7.4.6 Key Considerations for Effective Lockdown Procedures

- **Clear Communication Channels:** Ensure communication systems, including PA systems and mass notification tools, are functioning properly and accessible to authorized personnel.
- **Rapid Lockdown Activation:** The ability to quickly initiate a lockdown is crucial. Ensure that panic buttons or electronic locking systems are well-maintained and operational.
- **Patient Considerations:** Always prioritize the safety of patients, particularly those who are vulnerable, immobile, or in critical care units.
- **Coordination with Law Enforcement:** Strong collaboration with local law enforcement is essential for effective lockdown management. Ensure that law enforcement is familiar with the hospital's layout and emergency procedures.

8 CYBERSECURITY

8.1 Introduction:

Cyber security refers to the practice of protecting systems, networks, and data from digital attacks, unauthorized access, damage, or theft.

In hospitals, cyber security plays a critical role in protecting:

- Patient health information (PHI) stored in Electronic Health Records (EHR).
- Financial data related to billing and insurance.
- Clinical systems used for diagnosing and treating patients.
- Operational systems that manage hospital services and infrastructure.

8.2 Significance of Cyber security in Protecting Patient Data

Healthcare facilities, such as hospitals, rely heavily on digital systems to manage patient care and administrative tasks. These systems contain sensitive personal health information (PHI), which is protected under various data protection laws like India's Digital Personal Data Protection (DPDP) Act, 2023. The significance of cyber security in this environment cannot be overstated, as cyber-attacks can have devastating consequences, including:

- **Patient Safety Risks:** A breach in a hospital's IT systems can lead to the alteration or loss of critical patient data, which could delay diagnoses or lead to incorrect treatment.
- **Data Breaches and Privacy Violations:** Healthcare organizations store large amounts of sensitive personal and medical data, making them prime targets for attackers looking to steal, sell, or ransom such information.
- **Financial Impact:** A successful attack could lead to significant financial losses due to ransom ware payments, downtime, and legal penalties for non-compliance with regulations.
- **Trust Erosion:** Cyber security breaches can damage a hospital's reputation, causing patients and partners to lose confidence in the institution's ability to protect their data.

Due to these risks, maintaining robust cyber security is essential for protecting patient privacy, ensuring uninterrupted healthcare services, and complying with legal requirements.

8.2 Network Security

8.2.1 Definition and Role of Network Security in a Healthcare Environment

Network security in hospitals refers to the policies, practices, and technologies used to safeguard the integrity, confidentiality, and availability of hospital networks and the sensitive data they carry. Hospitals rely on interconnected systems such as Electronic Health Records (EHR), medical devices, patient monitoring systems, and administrative platforms, making network security a critical component of overall hospital cyber security. The role of network security in a healthcare environment includes:

- **Protecting patient data:** Ensuring the privacy of sensitive personal health information (PHI)
- **Preventing unauthorized access:** Securing hospital systems from external attackers and internal threats
- **Ensuring continuity of care:** Keeping critical systems, such as diagnostic tools and EHRs, online and functional
- **Complying with regulatory requirements:** Adhering to laws like India's Digital Personal Data Protection (DPDP) Act, the Information Technology (IT) Act, and healthcare guidelines, which mandate specific security measures to protect personal and medical data

8.2.2 The Concept of Layered Security and Its Application in Hospitals

Layered security, also known as the "defence in depth" strategy, involves implementing multiple layers of security measures across different points of the hospital's IT infrastructure. The idea is that if one layer is breached, the other layers still provide protection, reducing the chances of a successful attack.

Key layers of security in a hospital setting include:

- **Physical security:** Controlling access to hospital servers and data centres using measures like biometric access controls, security cameras, and key cards
- **Network security:** Firewalls, IDS/IPS systems, and VPNs
- **Endpoint security:** Protecting individual devices (such as computers, tablets, and IoT devices) with antivirus software, encryption, and secure configurations
- **Application security:** Ensuring hospital applications are free from vulnerabilities and using secure development practices
- **User training and access control:** Ensuring that staff members are aware of cyber security best practices and limiting access to sensitive systems based on role and necessity

In hospitals, layered security is particularly important because of the variety of systems and devices connected to the network. An attacker who gains access through a vulnerable medical device might be stopped by another security layer before reaching critical patient records.

8.2.3 Security Operations Center (SOC) in Hospitals

A Security Operations Center (SOC) plays a critical role in ensuring real-time monitoring, detection, and response to cyber security threats in hospital environments. A SOC is a centralized facility where security professionals' use advanced tools and processes to oversee and defend the hospital's IT infrastructure, including medical devices and sensitive data systems.

- **Real-time threat monitoring:** A SOC continuously monitors hospital networks for potential threats, allowing IT teams to detect and respond to incidents as they occur.
- **Incident response:** The SOC coordinates swift actions to contain, mitigate, and remediate incidents, reducing the risk of data breaches or disruptions in hospital operations.
- **Threat intelligence:** SOC teams collect and analyze threat intelligence to stay ahead of emerging cyber security risks, ensuring the hospital's defenses are aligned with the latest attack vectors.
- **Collaboration with IT staff:** SOCs work closely with hospital IT teams to enhance security across systems, address vulnerabilities, and implement best practices for cyber security resilience.

Incorporating a SOC helps hospitals strengthen their ability to respond to cyber threats in real time, minimizing the impact of attacks and ensuring continuous monitoring and protection of hospital networks and critical assets.

8.2.4 Monitoring and Logging Network Activity

Monitoring and logging network activity are crucial for detecting, investigating, and mitigating cyber threats. Hospitals must ensure continuous monitoring of network traffic, access logs, and system events to identify potential security incidents. Logs provide detailed records of user activity, device access, and data flow, helping IT staff detect anomalies such as unauthorized access attempts or suspicious data transfers.

Best practices for monitoring include:

- **Implementing centralized logging systems:** Collect and store log data from multiple sources, such as firewalls, servers, and applications, in a single location for easier analysis
- **Using Security Information and Event Management (SIEM) systems:** Automate the process of log analysis, correlating data across systems to identify potential threats
- **Setting up alerts for suspicious activities:** Immediate notifications for abnormal activities, such as repeated failed login attempts or unexpected large data transfers, can help quickly mitigate threats
- **Regularly auditing logs:** Conduct periodic reviews of log data to detect patterns or anomalies that may indicate a security threat or a vulnerability

8.2.5 Best Practices for Network Security

Hospitals can adopt a range of best practices to enhance network security and reduce the risk of cyber-attacks:

- **Regular software updates and patch management:** Ensure that all systems, including medical devices, are kept up to date with the latest security patches to prevent exploitation of known vulnerabilities
- **Network segmentation:** Divide the hospital network into segments based on function or sensitivity (e.g., separating administrative systems from medical devices) to limit the spread of malware or unauthorized access across the entire network
- **Multi-factor authentication (MFA):** Require additional authentication factors, such as biometric verification or one-time passcodes, for accessing sensitive hospital systems
- **Secure device management:** Implement strict policies for using and securing mobile devices, IoT devices, and laptops connected to the hospital network, such as mandatory encryption and antivirus software
- **Role-based access control (RBAC):** Limit user access to only the systems and data necessary for their specific job function, reducing the likelihood of unauthorized access
- **Data encryption:** Apply encryption to both data at rest and in transit to ensure that sensitive patient information is protected even if it is intercepted or stolen.

8.3 Data Protection

8.3.1 Definition of Data Protection in Hospitals

Data protection in hospitals refers to the implementation of policies, procedures, and technologies that safeguard sensitive information from unauthorized access, loss, or corruption. The goal of data protection is to ensure that sensitive information is handled with confidentiality, integrity, and availability, adhering to regulatory requirements and safeguarding patient trust.

8.3.2 Types of Sensitive Data

The types of sensitive data typically handled in hospitals include:

- **Patient Records:** This is the most sensitive type of data handled by hospitals including Electronic Health Records (EHRs). It includes personal identification information (such as names, addresses, and contact details), medical history, diagnoses, test results, treatment plans, and medication information.
- **Financial Data:** Hospitals collect financial information such as patient billing details, payment histories, insurance claims, and other transactional data.
- **Staff Information:** Employee records, including personal information, payroll data, and professional credentials, also need to be secured.

8.3.3 Data Protection Strategies

Hospitals must adopt comprehensive data protection strategies to mitigate risks and ensure compliance with legal requirements. Some of the key strategies include:

- **Data Encryption:** Encryption ensures that sensitive data is protected by converting it into an unreadable format that can only be decrypted by authorized parties with the correct encryption key. This is essential for protecting both stored data and data in transit.

- Encryption at rest: Ensures that sensitive data, such as patient records stored in databases, is encrypted and remains protected even if unauthorized individuals gain access to the storage systems.
- Encryption in transit: Encrypts data as it moves between systems, departments, or remote locations to prevent interception by unauthorized parties.

- **Secure Storage and Backup Procedures:** Regular backups and secure storage mechanisms are essential to protect hospital data from loss, corruption, or ransomware attacks. Hospitals should:
  - Maintain **redundant backups** in multiple secure locations to ensure data can be restored in the event of hardware failure or a cyberattack.
  - Implement **cloud-based storage** solutions with encryption and access controls for offsite data backups.
  - Ensure that backup data is stored in compliance with data protection regulations and that it is regularly tested for integrity and recovery speed.
- **Access Control Policies:** Access control policies regulate who can access certain types of data and ensure that only authorized personnel can view, edit, or share sensitive information. Effective access control involves:
  - Implementing role-based access control (RBAC) to grant employees access based on their job roles and responsibilities, reducing the risk of unauthorized access to sensitive data.
  - Using multi-factor authentication (MFA) to add an extra layer of security, requiring users to provide multiple forms of verification before accessing critical systems.
- **Role-Based Access Control (RBAC):** RBAC restricts access to sensitive information based on the user's role within the hospital. For example, doctors may have access to patient health records, but administrative staff may only have access to patient contact information. RBAC helps reduce the risk of insider threats and ensures that employees can only access the data they need for their specific job functions.

8.3.4 Relevant Indian Data Protection Laws

In India, several laws and regulations govern the protection of sensitive data, particularly in healthcare. Hospitals must ensure compliance with these laws to protect patient privacy and avoid legal penalties.

- **Digital Personal Data Protection (DPDP) Act, 2023:** The DPDP Act establishes a legal framework for the protection of personal data in India. It sets out the rights of individuals (data principals) and the responsibilities of organizations (data fiduciaries) in handling personal data. Key provisions relevant to hospitals include:
  - Hospitals must obtain consent before collecting or processing personal data.
  - Sensitive personal data, including health data, must be processed in compliance with strict privacy and security guidelines.
  - Hospitals must implement adequate security measures to protect personal data and notify authorities in case of data breaches.

- Data must be stored only for as long as necessary and used only for its intended purposes.
- **Link:** https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf

- **Information Technology (IT) Act, 2000:** The IT Act is India's primary legislation governing the use of electronic records and digital transactions. Specific sections of the IT Act are particularly relevant to healthcare data protection:
  - **Section 43A:** Organizations that handle sensitive personal data must implement reasonable security practices and procedures. If an organization is negligent in maintaining these security measures, resulting in a data breach, it can be held liable for damages.
  - **Section 72:** Imposes penalties on individuals or organizations that disclose personal information without the consent of the person to whom the information belongs.
  - **Link:** https://www.meity.gov.in/content/information-technology-act-2000-0
- **Health Ministry Guidelines:** The Ministry of Health and Family Welfare in India also provides guidelines on the management of health data and the adoption of electronic health records (EHR). These guidelines include best practices for ensuring data privacy, security, and interoperability of health systems.
  - **Link:** https://esanjeevani.mohfw.gov.in/assets/guidelines/ehr_guidlines.pdf

8.3.5 Ensuring Compliance with Data Protection Regulations

Hospitals must not only implement technological solutions for data protection but also develop policies and procedures that align with India's legal framework. Steps for ensuring compliance include:

- Conducting regular data protection impact assessments (DPIA) to evaluate the risks associated with processing sensitive data and ensuring that appropriate security controls are in place.
- Implementing privacy policies that outline how patient data will be collected, stored, and shared. These policies should be made available to patients, and consent should be obtained where required by law.
- Establishing incident response plans to quickly identify, contain, and report data breaches to the relevant authorities as mandated by law.
- Regularly auditing data protection measures to ensure that they meet the evolving legal and regulatory requirements, and that all staff are trained on data protection responsibilities.

8.4 Handling Cyber security Threats

8.4.1 Types of Cyber security Threats in Hospitals

Hospitals, as custodians of sensitive data and critical medical systems, are frequent targets for various types of cyber-attacks. Understanding these threats is crucial for developing effective defensive strategies. Below are the most common types of cyber security threats hospitals face:

- **Ransom ware:** Ransom ware is a type of malicious software designed to block access to data or systems until a ransom is paid. In hospitals, ransom ware can cripple operations by locking access to patient records, diagnostic tools, or administrative systems, making it impossible to provide critical care. Attackers often demand payment in crypto currency to restore access to the affected systems.
- **Phishing:** Phishing is a social engineering attack in which cybercriminals trick hospital staff into providing sensitive information, such as login credentials, by posing as legitimate entities. Phishing attacks are typically conducted through deceptive emails or messages that mimic trusted sources like other healthcare providers, insurance companies, or internal communications.
- **Malware:** Malware refers to any malicious software that infiltrates hospital systems to cause harm, steal information, or gain unauthorized control. Common types of malware include viruses, worms, trojans, and spyware.
- **Insider Threats:** Insider threats come from employees, contractors, or partners who have legitimate access to hospital systems but misuse their access for malicious purposes or due to negligence. Insider threats are especially dangerous because insiders already have trusted access to sensitive data, making it harder to detect malicious activity.
- **Social Engineering Attacks:** Social engineering attacks manipulate hospital staff into divulging confidential information or performing actions that compromise security. In hospitals, social engineering can take the form of impersonation (e.g., pretending to be IT staff to gain access to systems) or inducing panic (e.g., a fraudulent emergency request for information).

8.4.2 Processes of Common Cyber security Attacks

Cyber-attacks on hospitals follow specific processes to exploit vulnerabilities and gain unauthorized access to sensitive data and systems. The following outlines the typical steps taken by attackers and how these processes affect hospitals.

- **Infection Vectors:** Infection vectors refer to the methods used by cybercriminals to introduce malware or gain unauthorized access to hospital systems. Common infection vectors include:
  - **Email:** Phishing emails containing malicious attachments or links are a common method for spreading malware or obtaining user credentials.
  - **USB drives:** Inserting compromised USB drives into hospital computers can introduce malware into the network.
  - **Third-party software:** Hospitals often rely on third-party software for various functions. Attackers may exploit vulnerabilities in these applications to gain access to hospital systems.
- **Steps Attackers Take to Exploit Vulnerabilities:** Once attackers have established a foothold in hospital systems through an infection vector, they follow a series of steps to further their attack:
  - **Reconnaissance:** Attackers gather information about the hospital's IT environment, identifying potential vulnerabilities or valuable targets such as patient records or financial data.

- **Exploitation:** Attackers use the information gathered during reconnaissance to exploit vulnerabilities, such as unpatched software, weak passwords, or misconfigured systems.
- **Privilege Escalation:** Once inside the system, attackers attempt to elevate their privileges to gain greater control over the network. This may involve exploiting flaws in access control systems or using stolen credentials.
- **Lateral Movement:** Attackers move laterally across the network to infect additional systems or access more sensitive data. This often involves using compromised user accounts or exploiting weak internal security controls.
- **Data Exfiltration or Disruption:** The final step involves stealing sensitive data (such as patient health records) or disrupting hospital operations (such as deploying ransomware). In some cases, attackers may destroy data or systems to cover their tracks or maximize damage.

8.4.3 Identifying Attack Patterns and Indicators of Compromise (IOC)

Hospitals must continuously monitor their networks for early signs of cyberattacks. Identifying attack patterns and Indicators of Compromise (IOC) can help detect and respond to security incidents before they cause significant damage.

- **Attack Patterns:** Attack patterns refer to the techniques, tactics, and procedures (TTPs) commonly used by cybercriminals. These patterns can include the methods used to gain access, escalate privileges, and move laterally within a network. By recognizing these patterns, hospitals can anticipate potential threats and respond proactively.

  Common attack patterns in hospitals include:

  - Repeated failed login attempts or suspicious login behavior (e.g., access from unusual locations or times)
  - Unusual data transfers or attempts to access large volumes of patient records
  - Installation of unauthorized software or unexpected system changes
  - Sudden spikes in network traffic that could indicate malware activity or data exfiltration
- **Indicators of Compromise (IOC):** Indicators of Compromise are artefacts or evidence left behind by attackers during or after a cyber-attack. Monitoring for these IOCs allows hospitals to detect potential breaches in real-time and respond before the attack progresses. Common IOCs in hospital environments include:
  - **Suspicious network traffic:** Unusual traffic patterns, such as outbound communication with known malicious IP addresses or large data transfers, can indicate data exfiltration or malware activity.
  - **Unauthorized access attempts:** Repeated login failures, particularly from external sources or at odd hours, can signal an attempted breach.
  - **Unusual system behaviour:** Slow system performance, unexplained crashes, or unexpected pop-up windows may be signs of malware infection or system compromise.
  - **Changes in file integrity:** Unauthorized modification of critical files or encryption of data may indicate a ransom ware attack or other malicious activity.

- **Anomalies in user activity:** Employees accessing data or systems outside of their regular roles or behaviour may indicate an insider threat or compromised credentials.

8.5 Staff Training on Cyber security Awareness

8.5.1 Importance of Cyber security Training for Hospital Staff

In healthcare, Cyber security training equips staff with the knowledge and skills needed to recognize threats, follow security best practices, and respond appropriately in the event of a breach. Ensuring that all hospital employees understand their role in protecting patient data and maintaining the integrity of hospital systems is critical to reducing cyber security risks.

8.5.2 Types of Cyber security Training

To be effective, cyber security training must be tailored to the specific roles and responsibilities of hospital staff.

- **General Awareness Training:** This type of training is provided to all staff and covers basic cyber security principles, including:
  - **Password Management:** Ensuring strong, unique passwords for different systems, avoiding password reuse, and enabling multi-factor authentication.
  - **Email Phishing Awareness:** Training staff to recognize phishing emails by looking for red flags like suspicious senders, grammar mistakes, unexpected attachments, or requests for personal information.
  - **Data Security:** Understanding the importance of keeping patient data secure and confidential, both digitally and physically.
- **Role-Specific Training:** Role-specific training ensures that hospital staff receives focused instruction on the cyber security challenges relevant to their job functions.
  - **IT Staff:** Advanced training on network security, data encryption, system monitoring, and incident response. IT staff should also receive training on regulatory compliance and be familiar with hospital cyber security frameworks like ISO 27001.
  - **Doctors and Nurses:** Training on how to securely access and manage Electronic Health Records (EHR), protect patient confidentiality, and recognize potential threats (e.g., malware on medical devices).
  - **Administrative Staff:** Training on how to securely handle sensitive patient and financial data, safeguard communications, and recognize social engineering attacks.
  - **Senior Management:** Training on the importance of implementing a strong cyber security culture, complying with regulations, and ensuring that proper security policies are in place and enforced.

8.5.3 Key Areas of Focus for Cyber security Training

Effective cyber security training programs should focus on specific areas that pose the highest risks to hospitals. Staff must understand how to protect sensitive information and recognize potential cyber threats.

- **Recognizing Phishing Attempts:** Phishing is one of the most common ways cybercriminals gain access to hospital systems. Key elements to cover under training include:

- Verifying email senders, even if the email looks legitimate
- Checking for warning signs such as grammar errors, unusual requests, or unexpected attachments
- Reporting suspicious emails to the IT department for further investigation

- **Safe Internet Browsing:** Hospital staff should be trained on how to browse the internet safely, including:
  - Avoiding untrusted websites and downloading unauthorized software or files
  - Recognizing malware warning signs, such as sudden pop-ups or system slowdowns
  - Using VPNs and secure browsing protocols, especially when accessing hospital systems remotely
- **Handling Sensitive Information Securely:** Hospitals handle large volumes of sensitive data daily, from patient health records to financial information. Training should emphasize:
  - Secure methods for storing, transmitting, and sharing sensitive data, including encryption and secure email systems
  - Ensuring physical security of devices containing sensitive information, such as laptops and mobile devices
  - Locking computer screens when away from the workstation and preventing unauthorized access to confidential data

8.5.4 Engaging Staff with Real-World Examples

One of the most effective ways to make cyber- security training relevant and engaging is to use real-world examples. By showing staff how cyber-attacks have impacted other hospitals or healthcare organizations, training can drive home the importance of vigilance.

- **Case Studies:** Presenting real-life examples of cyber- security incidents in healthcare, such as ransom ware attacks or data breaches, helps staff understand the potential consequences of cyber threats. These case studies should include details about how the attack occurred, its impact, and how it could have been prevented.
- **Interactive Scenarios:** Simulated attack scenarios can make training more interactive and memorable. For example, running a phishing simulation in which staff receives emails that mimic real phishing attempts and must determine whether the emails are legitimate or malicious.
- **Gamification:** Incorporating game-like elements into training, such as quizzes, challenges, or leader boards, can boost engagement and motivation. Staff can earn points or badges for correctly identifying threats or completing training modules, encouraging a competitive but educational atmosphere.

8.6 Collaboration with IT Department

8.6.1 Importance of Constant Communication between Healthcare and IT Teams

Effective collaboration between healthcare teams and the IT department is essential for a hospital's cyber- security strategy. The importance of this communication can be understood in several ways:

- **Understanding security needs:** Healthcare teams handle sensitive patient data and medical devices, so they must regularly communicate with the IT department to convey their security needs and challenges.
- **Raising security awareness:** IT teams must work closely with healthcare staff to raise awareness of common cyber- security threats, such as phishing attacks and malware.
- **Identifying potential vulnerabilities:** Healthcare professionals may encounter security risks, such as outdated software or improperly configured devices. Regular communication with IT can help address these vulnerabilities before they become major problems.
- **Collaborative problem-solving:** Cyber- security is a shared responsibility. When healthcare teams encounter suspicious activity, they should report it immediately to IT for investigation. Quick and effective communication can prevent a minor issue from escalating into a major security breach.

8.6.2 Technical Support during a Cyber- security Incident

When a cyber- security incident occurs, the IT department is at the forefront of the response. Technical support during a cyber- security incident includes the following key actions:

- **Incident identification and classification:** IT teams use monitoring tools to detect abnormal activity or indicators of compromise (IOCs). Once a potential incident is detected, they must determine its nature (e.g., phishing, ransom ware, or data breach) and severity to prioritize response efforts.
- **Containment:** Once an incident is identified, the IT department works to contain it by isolating affected systems. For example, if ransom ware infects a part of the network, IT staff may disconnect the infected systems from the broader hospital network to prevent further spread.
- **Eradication:** After containment, the IT department works to remove the threat, such as disinfecting malware, patching vulnerabilities, or stopping unauthorized access. Eradication efforts are crucial for restoring the hospital's cyber- security defenses.
- **Data recovery and system restoration:** IT teams are responsible for restoring affected systems, often by recovering data from backups. Ensuring that patient care can continue with minimal disruption is a critical focus during the recovery process.
- **Communication and coordination:** During an incident, the IT department must keep hospital leadership and relevant departments informed of the incident's status. Healthcare teams need updates on which systems are affected and when they can expect normal operations to resume.
- **Post-incident review:** After the immediate threat is addressed, IT teams conduct a thorough review of the incident to determine its root cause, evaluate the effectiveness of the response, and implement lessons learned to prevent future incidents.

8.6.3 Collaborating on Security Policies, Audits, and Compliance Measures

The collaboration between hospital leadership, clinical teams, and IT is essential for establishing strong cyber- security policies, conducting regular audits, and ensuring compliance with legal regulations.

- **Developing security policies:** IT and healthcare teams should collaborate to create and update hospital-wide security policies that cover areas like password management, data access, mobile device usage, and incident reporting. Policies must be aligned with operational needs and regulatory requirements, such as those set by the DPDP Act and IT Act in India.
- **Conducting security audits:** Regular security audits help identify gaps in cyber- security practices. Collaboration between the IT department and hospital management is crucial for ensuring that audits are thorough and that any identified vulnerabilities are promptly addressed.
- **Compliance measures:** Hospitals must comply with various cyber- security regulations, including the DPDP Act, which governs the protection of personal data, and international standards like ISO 27001. IT teams play a critical role in ensuring compliance by implementing the necessary controls.
- **Training and awareness:** IT departments should collaborate with human resources and hospital management to ensure that all staff receive regular cyber- security training.

(Note: More detail on cyber- security is annexed as annexure-1)

9 HANDLING SPECIFIC THREAT

9.1 Active Shooter Protocol

9.1.1 Introduction: An active shooter protocol in a hospital setting focuses on ensuring the safety of patients, staff, and visitors while minimizing casualties. Like healthcare institutions worldwide, hospitals in India must be prepared to handle such incidents. The following protocol aligns with best practices for managing active shooter scenarios in hospitals, referencing applicable Indian laws and guidelines.

9.1.2 Immediate Response: When an active shooter is identified, immediate action must be taken to minimize harm. This can include Run, Hide, and Fight, a widely recognized approach used in many countries, including India.

a. **Run: Evacuate if Possible**

- Evacuation is the priority if it's safe. Staff should:
  - Help ambulatory patients and visitors evacuate.
  - Direct individuals away from the shooter's location using the closest, safest exits.
  - Follow evacuation routes already designated in the hospital's disaster management plan.
  - Avoid elevators, and leave personal belongings behind.

Alert Authorities:

- Call the police (**Dial 100**) and provide the following:
  - Shooter's location.
  - Description of the shooter(s), including weapons.
  - Number of shooters, if possible.
  - Number of potential victims.

b. **Hide: Shelter in Place**

If evacuation isn't possible, staff should take cover:

- Find a Secure Location:
  - Stay out of sight, ideally behind a locked door or in a room with barricades.
  - Turn off lights, silence mobile phones, and remain quiet to avoid drawing attention.

- **Lock and Barricade:**
  - Lock doors and use heavy objects (furniture, beds, etc.) to block entry.
- **Remain Calm and Communicate:**
  - Notify law enforcement about your location if possible, via text message or silent communication methods.

c. **Fight: Last Resort**

As a last resort, when lives are in immediate danger, it may be necessary to confront the shooter.

- **Engage with Aggression:**
  - Improvise weapons from nearby objects (chairs, medical equipment).
  - Aim to disarm or incapacitate the shooter.

9.1.3 Alert Hospital Authorities:

The individual who identifies the shooter must also:

a. **Activate the Hospital Emergency Code:**

- Use internal communication channels to announce an active shooter. Some hospitals may use **Code Silver** for armed individuals.

b. **Trigger Lockdown Procedures:**

- The hospital's security team should immediately lock down entry and exit points.
- Coordinate with local law enforcement and hospital leadership.

9.1.4 Coordination with Law Enforcement:

Upon arrival, local law enforcement will take charge of the situation.

a. **Provide Information:**

- Security and staff should provide law enforcement with details on the shooter's location, entry points, and hospital layout.

b. **Assist Authorities:**

- Cooperate fully with police, military, or other government agencies who may be involved in neutralizing the threat.

c. **Bomb Squad or Special Units:**

- In case of threats involving explosives, law enforcement may deploy bomb squads or special units like the National Security Guard (NSG).

9.1.5 Protect Patients and Critical Areas:

While staffs are securing themselves and others, attention must also be given to patients, particularly those in vulnerable situations (ICUs, OTs, etc.).

a. ICU, OT, and Neonatal Units:

- These areas should remain locked down, and staff should secure doors, close blinds, and create a fortified area around critical patients.

b. **Non-Ambulatory Patients:**

- Prioritize hiding or sheltering non-ambulatory patients in rooms that can be locked or barricaded.

c. **Evacuating Critical Patients:**

- If evacuation becomes possible, coordinate with law enforcement to move critical patients to safe zones outside the hospital, such as pre-designated assembly points.

9.1.6 Communication and Information Control:

During an active shooter event, controlling the flow of information is critical to avoid panic and misinformation.

a. **Internal Communication:**

- Use hospital PA systems, mobile apps, or intercoms to update staff without creating panic.

b. **External Communication:**

- The hospital's Public Relations Officer (PRO) or media spokesperson should handle all external communication, ensuring that accurate, non-sensitive information is released.

c. **Social Media Monitoring:**

- Actively monitor social media to manage false information or rumors, as panic can spread quickly through these platforms.

9.1.7 After the Incident:

Once the situation is resolved, the hospital must focus on recovery and ensuring the safety of everyone involved.

a. **Secure the Area:**

- Law enforcement will secure and clear the building before allowing anyone back into the facility.

b. **Medical and Psychological Support:**

- Provide **medical assistance** to any injured individuals.
- Arrange for **counseling services** for staff, patients, and families who may have been traumatized by the event.

c. **Post-Incident Review:**

- Conduct a **debriefing session** with hospital management, law enforcement, and security personnel to identify lessons learned and potential improvements to the hospital's active shooter protocol.

d. **Documentation:**

- Prepare a detailed incident report, including actions taken, casualties (if any), and areas for improvement.
- Report the incident to **state health authorities** and, if applicable, **accreditation bodies** (e.g., NABH).

9.1.8 Training and Drills:

Hospitals must regularly train staff and conduct mock drills to ensure preparedness for active shooter scenarios.

a. **Regular Training:**
   - All staff should receive training on recognizing gunfire, response protocols, and communication during an active shooter event.

b. Mock Drills:
   - Conduct **annual or semi-annual drills** simulating an active shooter event, in coordination with local police and emergency services.

c. Security Infrastructure:
   - Evaluate the hospital's **security measures** (CCTV coverage, emergency communication systems, secures access points) and upgrade them as needed.

9.2 Bomb Threat Protocol

9.2.1 Introduction: Bomb threat management in hospitals is critical to ensuring patient safety, staff well-being, and continuity of medical services. In India, as in other countries, the handling of bomb threats in healthcare facilities must follow well-established protocols, which should be integrated into the hospital's disaster management plan. Below is a step-by-step protocol tailored for hospitals in India, taking into account local authorities, resources, and security practices.

9.2.2 Immediate Response:

When a bomb threat is received, it should be treated with seriousness, irrespective of whether the threat seems credible or not.

a. **Record the Threat:**
   - If the threat is received via phone, the receiver should remain calm, listen carefully, and note key details such as the caller's tone, background sounds, specific details about the threat, and the time of the call.
   - Use a **bomb threat checklist** (standardized forms should be available at hospital communication centers) to document the conversation.

b. Inform Authorities:
   - Notify the **local police (Dial 100)** immediately and provide them with all available information.
   - Inform the **hospital's security team** to activate internal protocols.

c. Alert the Hospital Management:
   - Immediately escalate the information to the Hospital Administrator, the Head of Security, and the Chief Medical Officer.
   - Prepare to inform all critical departments discreetly.

9.2.3 Evacuation Decision:

The decision to evacuate the hospital must be made with careful consideration of patient safety.

a. **Assess Threat Credibility**:
   - In coordination with local authorities, assess the credibility of the threat.
   - Authorities may send a **bomb disposal squad** or conduct a preliminary search to verify the threat.

b. **Partial or Full Evacuation**:
   - If the threat is deemed credible, hospital management, in consultation with law enforcement, will decide whether to:
     - **Evacuate partially:** Evacuate non-critical patients and staff first, followed by sensitive areas like Intensive Care Units (ICUs), Operating Theaters (OTs), and Neonatal Units.
     - **Full evacuation:** If necessary, move all patients and staff to a pre-determined safe location.
   - Evacuation plans should account for critical patients, ensuring that ventilators, monitors, and other essential equipment are available in the safe areas.

c. **Minimize Panic**:
   - Ensure communication with staff and patients is calm, clear, and avoids inciting panic.

9.2.4 Search and Sweep Operations:

Once authorities are informed, the hospital's security team and law enforcement agencies will initiate search protocols.

a. **Internal Security Sweep**:
   - Train the hospital's security personnel to conduct initial sweeps of areas such as emergency exits, public waiting areas, parking lots, and the hospital perimeter.

b. **Involvement of Law Enforcement**:
   - The bomb squad will handle the detailed search. Assist them by providing access to all hospital areas.
   - Cooperate with disaster management authorities (e.g., National Disaster Response Force, NDRF) if involved.

c. **Use of Equipment**:
   - Authorities may use sniffer dogs, bomb detection equipment, and other tools to locate any suspicious packages.

9.2.5 Communication Management:

Effective communication during a bomb threat ensures that misinformation is avoided, and patients remain safe.

a. **Internal Communication**:
   - Use internal communication channels (PA systems, internal messaging apps) to update staff regularly.
   - Inform staff on how to guide patients and visitors safely.

b. External Communication:

- A designated **Public Relations Officer (PRO)** or **media spokesperson** should handle external communication, including interactions with the media.
- Avoid releasing sensitive or speculative information until verified by authorities.

9.2.6 Handling of Suspicious Items:

If a suspicious item is found:

- Do Not Touch the item or package.
- Evacuate the immediate area and mark it for law enforcement.
- Inform the police and bomb squad immediately.

9.2.7 Post-Incident Actions:

Once the threat is neutralized:

a. **Post-Evacuation Safety:**

- Authorities must declare the hospital safe before re-entry is allowed.
- Conduct a headcount of staff and patients to ensure no one is missing.

b. **Review and Debrief:**

- Hold a **post-incident review meeting** involving hospital management, security staff, and law enforcement to discuss what went well and what can be improved.
- Provide **counseling** to staff and patients affected by the stress of the incident.

c. **Documentation:**

- Ensure detailed documentation of the incident, including timelines, actions taken, and outcomes.

d. **Report to Health Authorities:**

- Submit a report to the **State or District Health Authorities** and, if necessary, other regulatory bodies such as the **National Accreditation Board for Hospitals (NABH)**.

9.2.8 Training and Drills:

Regular training sessions and mock drills should be conducted to ensure preparedness.

a. **Staff Training:**

- All hospital staff should undergo training on bomb threat protocols, communication, and evacuation procedures.

b. Mock Drills:

- Conduct **annual or bi-annual drills** in coordination with local police and emergency services.

c. Emergency Resources:

- Ensure access to critical supplies like **emergency evacuation kits, medical supplies**, and **patient transport equipment**.

9.2.9 Legal Aspects in India:

- The Explosives Act, 1884 and The Disaster Management Act, 2005 in India provide the legal framework for handling such threats.
- Hospitals may need to coordinate with local disaster management authorities in accordance with the National Disaster Management Guidelines.

9.3 Fire Safety and Evacuation Procedures

9.3.1 Introduction: hospitals are designed to protect patients, staff, and visitors in the event of a fire or other emergencies. Hospitals, as infrastructures, contain extensive electrical wiring, heat-dissipating equipment, combustible gases and fuels, and chemicals. All of these elements are prone to hazardous incidents if proper precautions are not taken during the planning and design of the facility.

Following are fire safety and evacuation procedure and protocols with references to Indian guidelines and frameworks.

9.3.2 FIRE PREVENTION MEASURES: The design of the hospital building and the types of materials used in its construction are important factors in preventing the rapid spread of fire, smoke, or fumes and in ensuring resistance to complete burnout, thereby helping to protect lives and property.

a. **Fire Resistant Walls and Floors:**

- Use of fire resisting element. Fire resistance of a constructional element is defined in minutes or hours e.g. 120 minute or 1 hour. Every wall opening should be protected with fire-resisting doors, having the fire rating of not less than 120 minute.
- In hospital buildings, openings in walls or floors which are provided for passage of cables, electrical wirings etc. must be protected by enclosure in the form of ducts / shafts with fire resistance rating of 120 minute.

b. **Compartmentation:**

- Generally, these fire compartments are separated from each other by compartment walls and compartment floors made of a fire-resisting construction which acts as a barrier to the spread of fire and smoke for a specific period of time.
- All floors should be compartmented with area of each compartment equal to 1800 m2.

c. **Electrical Installation:**

- In hospital buildings, critical electrical cables must continue to function during a fire because electrical supply is essential for areas such as the ICU, operating theatres, and patient wards, where continuous patient health monitoring is required.
- Electrical cables / wiring should be laid in separate shaft and should have flame retardant property.
- Emergency power supply should be provided to the following equipment / systems:

- Pressurization and smoke venting; including its ancillary systems such as dampers and actuators.
- Fire pumps
- Fireman's lifts
- Exit signage lighting
- Emergency lighting
- Fire alarm system
- Public address (PA) system (relating to emergency voice evacuation and annunciation).
- Magnetic door hold open devices
- Lighting in fire command centre and security room.
- In hospital buildings, the substation / switch station with oil filled equipment should be located at least 7 meter away from the adjoining buildings.

d. **Diesel generator (DG)** set must not be installed on ground floor / first basement of the hospital buildings.

- The DG set if installed indoor, proper ventilation and exhaust should be planned.
- The DG set rooms should have 120 minute fire resistance rating.

e. Lightning protection of the hospital buildings should be ensured by routing of down conductors (insulated or uninsulated) through electrical shafts.

f. Air Conditioning, Ventilation and Smoke Control

- In hospital buildings, separate Air Handling Unit (AHU) should be provided for each floor so as to avoid the hazards arising from spread of fire and smoke through the air conditioning ducts.
- The air ducts should be separate from each AHU to its floor and in no way should interconnect with the duct of any other floor.
- In hospital buildings, air ducts serving main floor areas, corridors, etc, should not pass through the exits/exit passageway/ exit enclosure.
- Wherever the ducts pass through fire walls or floors, the opening around the ducts should be sealed with material having the fire resistant rating of the compartment.
- Fire or Fire/smoke dampers should be provided in supply air ducts, fresh air and return air ducts/ passages.
- Damper should be accessible to maintain, test and also replace, if so required. There should also be provision for manual operation of the dampers.

g. **Escape Lighting**

- Exit access, exits and exit discharge should be properly identified and continuously illuminated. Emergency lighting should be provided from an independent source i.e. from different source supplying normal lighting.
- The horizontal luminance at the floor level on the escape route must be not less than 10 lumens / m2. The emergency lighting should be provided to be put on within 5 second of the failure of the normal lighting supply and should be able to maintain the required illumination level for a period of not less than 90 minutes.
- The emergency lighting system should be well maintained and periodically inspected and tested.

h. **Exit Signage**

- The green colour illuminated exit sign indicating the direction should be installed in all direction and should be positioned so that no point in the exit access is more than 30 meters away from view.
- Additionally, each floor landing should have prominently displayed floor indicator boards showing the floor number.
- The sizes and colours of the exit signs should be in accordance with IS 9457, IS 12349, IS 12407.

i. **Life Safety Measures**

- The life safety measures in a hospital building mainly consist of means of egress requirements, compartmentation, smoke control systems, Gas supply systems, fire detection and alarm system, Fire drills, fire orders, lifts.

j. **Egress Requirements**

- Egress encompasses three key components: exit access, exits, and exit discharge.
- The maximum travel distance from any point within the building to a final exit should not exceed the limits mentioned in NBC 2016 (Part IV).
- Minimum height of doorway should be 2 meter (height), the width of door should depend on the number of patients beds kept in the room.
- Basement should not be used to store flammable or pathological or other laboratories particularly involving use of chemicals.
- The activation of the building automatic sprinkler system or fire detection system should automatically unlock the access control system.
- For hospital building, width of the corridor and aisle through which patient are moved should be minimum 2.4 meter.
- Wherever there is central corridor, which is part of exit access, the doors of rooms must open inwards.
- The floor surface of the corridor should not be inclined at a gradient steeper than 1 in 12 to the horizontal.

k. **Staircase**

- All hospital buildings must have minimum 2 staircases made of non-combustible material. Internal staircase should not be arranged around a lift.
- The preferred rise for each step should be not more than 150 millimeter, and the tread 300 millimeter and there should be between maximum 12 riser per flight.
- Lift must not open inside a staircase.
- The minimum width of the internal staircase must be 2 meter. Handrail must not project more than 90 millimeter.

l. **Ramps:**

- In hospital buildings, ramp width should not decrease along the direction of travel and slope should not exceed 1 in 12 inch.
- The width of the ramps through which patient are moved should be minimum 2.4 meter.
- The ramps should be provided with handrails on both sides.

m. **Lift**

- Lift should not be used in case of emergency by any occupants of the hospital premises.
- The stretcher lift in a lift bank should also act as fireman lift in event of emergency.

n. **Fire Lift**

- To ensure that fire service personnel can access upper floors with minimal delay, at least one lift should be designed for exclusive use by firefighters during emergencies.

o. **Smoke Control Systems**

- In hospitals smoke control can be ensured by effective pressurization system.
- The air intake ducts should be located 5 meter away from the smoke exhaust ducts. Smoke exhaust system must ensure atleast 12 air changes per hour in the area affected by fire / smoke.

p. **Gas Supply**

- The gas pipelines should always run in separate shafts and shafts should run on external walls and away from staircases.
- Emergency valves to shut off the gas supply connection should be located in accessible location.
- Wherever gas cylinder manifold is installed in the hospital premises, same should be adequately ventilated.
- Kitchens working on the LPG fuel should not be located in basements.

q. **Fire Detection and Alarm System**

- The fire detection and alarm system in building should be programmed with fire alarm panel to operate smoke control systems, hold up of the fire doors, visual and audible waning systems etc.
- In buildings provided with automatic fire alarm system, following must be monitored:
  - Water level in tanks
  - Hydrant and sprinkler pressures of respective zones as provided
  - Pump “ON/OFF” status

Manual Operated Electronic Fire Alarm System (MOEFA):

- MOEFA systems include the manual call points, talk back system and public address systems installed in the hospital buildings.
- The purpose of the MEOFA systems is to provide early warning to the occupants

r. **Tanks for Water Storage**

Underground Static Fire Water Storage Tank:

- The fire water tanks should be filled to the complete capacity and maintained on 24 x 7 bases.

- Water should be stored in two or more interconnected compartments of equal size to facilitate cleaning and maintenance.

Terrace Tank over respective towers:

- The fire water tanks should be filled to the complete capacity and maintained on 24 x 7 bases.
- Water should be stored in two or more interconnected compartments of equal size to facilitate cleaning and maintenance.

s. **Fire Water Pumps**

- The fire water pump house should be separated by fire wall all around and doors should be protected by fire doors (120 minute) rating.
- The fire water pump house should not have negative suction arrangement and submersible pumps should not be used.

t. **Fire Protection Measures**

The fire protection measures as per NBC 2016 to be considered for the hospital buildings may include the following:

Fire Extinguishers:

Fire extinguishers are the first line of defence against a fire. Fire extinguishers should be installed throughout the hospital premises. Fire extinguishers should be mounted at a convenient height.

First Aid Hose Reel:

- The first aid hose reel should be installed on the downcomers / wet risers installed in the hospital premises.
- Minimum diameter of the hose reel should not be less than 19 mm.

Wet Risers:

- An arrangement of fire fighting in the building by means of vertical fire water line with diameter not less than 100 millimeter and fire hydrant valves on each floor / landing.
- Wet risers are permanently charged with water.
- The pressure available at the hydrant points should be between 3.5 to 7 bar.

Yard Hydrant:

- A network of fire hydrant installed in the premises outside the hospital building.
- The pressure in the yard hydrants should not exceed 7 bar.

Automatic Sprinkler System:

- Automatic sprinklers should be installed in all areas except in substation and DG set area.
- Pressure in sprinkler system should not exceed 12 bar.
- Provision should be made to ensure water from sprinkler do not enter the lift and electrical rooms.

9.3.3 Fire and Emergency Drill Planning And Preparation

a. **Plan Mock Drill Regularly**

- It should be conducted in every 3-6 months and at end of drill collect feedback from participants.
- Conduct debriefing session and assess how well the procedures were followed and identify any issues/weaknesses.
- Assess for evacuation planning and procedures, exit routes and signage etc

b. **Inspection of Building for Fire Safety**

- **Review Building Plans:** Understand the layout, fire escape routes, and location of fire safety equipment.
- **Gather Equipment:** Have a checklist, a flashlight, a camera, and any necessary measuring tools.
- **Exterior Inspection:** Ensure that fire lanes are clear and accessible. Verify that fire department access points are not obstructed.
- **Electrical Safety :** Check for electrical cords and outlets, all electrical panels should be accessible and labelled
- **Additional Hazards:** Check for any hazardous materials or processes on site, are there any open flames or sparks (e.g., welding, candles)

c. **Regular Maintenance**

- Regular checks of fire safety equipment, exit routes, and emergency systems to ensure they are in working order. Ensuring that all safety systems, including alarms, sprinklers, and emergency lighting, are properly maintained and serviced.

9.3.4 Evacuation Procedures

- **Preparation and planning:**
  - **Emergency Plan:** Develop and maintain a comprehensive emergency evacuation plan tailored to the specific needs and layout of the building.
  - **Designated Routes:** Identify and clearly mark evacuation routes, exits, and assembly points.
  - **Roles and Responsibilities:** Assign specific roles and responsibilities to staff, including evacuation coordinators, fire wardens, and first aid personnel.
- **Alarm systems:**
  - **Detection:** Ensure that fire alarms, smoke detectors, and other alert systems are functional and strategically placed.
  - **Notification:** Activate alarms to alert occupants of the emergency and initiate the evacuation process.
- **Immediate actions:**
  - **Alert and Notify:** Use alarms and public address systems to inform everyone of the emergency.
  - **Initiate Evacuation:** Begin the evacuation process, guiding occupants to follow established routes to safety.

- **Evacuation procedures:**
  - **Clear Communication:** Use clear, calm, and concise communication to direct people to the nearest exits and assembly points.
  - **Assistance:** Provide assistance to individuals with mobility issues, including the use of evacuation chairs or other aids if needed.
  - **Evacuation Routes:** Ensure that evacuation routes are unobstructed and clearly marked. Avoid using elevators if there's a fire.
- **Assembly points:**
  - **Designated Areas:** Direct evacuees to predetermined assembly points outside the building where they can be accounted for and receive further instructions.
  - **Accountability:** Verify that everyone has evacuated and is present at the assembly points.

9.3.5 Post-Evacuation Actions:

- **Assessment:** Evaluate the effectiveness of the evacuation and address any issues encountered.
- **Provide Medical and Psychological Support:** Provide medical assistance and psychological support to those affected by the evacuation.
- **Debriefing:** Conduct a debriefing session to review the evacuation process, identify any areas for improvement, and update procedures as needed.

9.4 Handling Aggressive or Violent Individuals

9.4.1 Introduction: Handling aggressive or violent individuals in hospitals, especially in a healthcare setting, requires well-structured protocols to ensure the safety of staff, patients, and visitors. In India, hospitals often face unique challenges due to high patient volumes, limited resources, and sometimes tense interactions between patients' families and hospital staff. Below is a protocol tailored for Indian hospitals, along with references specific to the Indian context.

9.4.2 Protocol for Handling Aggressive or Violent Individuals in Hospitals

a. **Assessing the Situation**

- **Remain Calm:** Hospital staff should remain calm and composed when confronted with aggressive behavior. The goal is to de-escalate the situation without triggering further violence.
- **Assess the Risk:** Quickly assess if the individual poses an immediate threat to themselves, others, or property. This involves recognizing verbal threats, physical postures, or other warning signs (e.g., loud yelling, pacing, aggressive body language).

b. **De-escalation Techniques**

- **Verbal De-escalation:** Trained staff should use communication techniques such as:
  - Maintaining a non-threatening posture.
  - Using a calm, steady tone of voice.

- Listening actively to the individual's concerns without interrupting or arguing.
- Offering solutions or alternatives to help resolve their issues.

- **Empathy:** Often, violent behavior stems from fear, frustration, or misunderstanding. Demonstrating empathy and acknowledging the individual's emotions can help diffuse tension.

c. **Involving Security**

- **Alert Security:** If the situation shows signs of escalating, staff should discreetly alert Hospital Safety and Security personnel.
- **Security Personnel Involvement:** Indian hospitals often have in-house security guards who can intervene to ensure the safety of hospital staff and other patients. They should try to escort the aggressive individual to a less populated area if safe to do so.

d. **Physical Restraint (Last Resort)**

- Physical restraint should only be used as a **last resort** when all other options have failed, and the individual poses an imminent threat. This should always be done following legal guidelines and in the presence of trained security personnel.

e. **Role of Local Law Enforcement**

- **Calling the Police:** In situations where the individual cannot be controlled by de-escalation or security measures, hospital administrators must involve local law enforcement to remove the individual and prevent harm.

f. **Emergency Action Plan (EAP)**

- **Activate Hospital Emergency Protocols:** If the situation escalates beyond immediate control, activate the hospital's emergency action plan.
  - Lockdown procedures may be required in extreme cases, isolating the violent individual from other parts of the hospital.
  - Ensure that patients in critical areas, such as the ICU or operating rooms, are protected from exposure to the situation.

g. **Managing Family and Visitors**

- **Control Crowds:** In India, large families often accompany patients to hospitals. In cases of aggression, crowd control becomes a critical issue. Hospital staff should maintain clear communication with the family members and use designated spaces for interaction (such as waiting areas) to avoid overcrowding sensitive zones.

h. **Legal Recourse**

- **Indian Penal Code (IPC) Sections on Violence in Hospitals:** Under IPC Section 186 (obstructing public servant in discharge of public functions) and IPC Section 332 (causing hurt to deter public servant), individuals involved in violence against hospital staff can be prosecuted.
- The Healthcare Service Personnel and Clinical Establishments (Prohibition of Violence and Damage to Property) Act, 2019, was introduced to protect

healthcare workers from violence and includes provisions for imprisonment and fines for perpetrators.

i. **Post-Incident Procedures**

- **Medical Care for Injured Staff or Patients:** If any injuries occur, ensure prompt medical care for affected individuals.
- **Report the Incident:** Document the incident, including witness accounts, the individual's behavior, steps taken to de-escalate, and any actions by law enforcement or security personnel.
- **Counseling for Affected Staff:** Hospital staff affected by violence may require mental health support or counseling to cope with the aftermath.

9.4.3 Training and Awareness

- **Staff Training:** Hospitals should conduct regular training programs for all staff on how to recognize signs of escalating aggression and how to safely manage violent situations.
- **Cultural Sensitivity Training:** Given the diverse cultural and socioeconomic backgrounds of patients in Indian hospitals, cultural sensitivity training can help staff communicate more effectively and reduce misunderstandings that might lead to aggression.

9.5 Security during Mass Casualty Events

9.5.1 Introduction: Security during mass casualty events (MCEs) is a critical concern for hospitals and healthcare facilities to ensure the safety of patients, staff, responders, and the general public while maintaining effective medical operations. In India, mass casualty events may include natural disasters (earthquakes, floods), terrorist attacks, industrial accidents, and pandemics. A well-structured protocol that incorporates security measures can prevent chaos, manage crowds, and protect hospital infrastructure.

9.5.2 Protocol for Hospitals during Mass Casualty

a. **Preparedness and Planning**

- Every hospital should have a disaster management plan integrated into its security framework. This plan should outline procedures for handling mass casualties, including triage, communication, and resource allocation.
- Regularly review and update the plan in line with guidelines from the National Disaster Management Authority (NDMA) and state-specific frameworks.

b. **Hospital Safety and Security Risk Assessment**

- Conduct a risk assessment to identify potential vulnerabilities, including hospital entry points, critical infrastructure (ICUs, surgical wards), and communication systems.
- Collaborate with local law enforcement to identify external threats and establish protocols for a coordinated response.

c. **Security Personnel Training**

- Train Hospital Safety and Security personnel in:
  - Crowd control
  - Handling aggressive individuals
  - Evacuation procedures
  - Use of communication devices in crisis situations
- Conduct drills and exercises involving hospital staff and local authorities to simulate MCEs and security responses.

d. **Activation of Mass Casualty Event Protocol**

- Activate the Incident Command System (ICS) to ensure a coordinated response.
- The ICS should include a Security Command structure responsible for managing:
  - Access control
  - Crowd management
  - Internal and external communication
  - Coordination with law enforcement and disaster management authorities.

e. **Communication and Coordination**

- Establish secure lines of communication between:
  - Hospital administration
  - Security teams
  - Medical teams
  - Law enforcement agencies
  - Disaster response teams (NDMA, NDRF)
- Use pre-established communication tools such as hospital radio networks, landlines, and dedicated mobile channels. Avoid using public networks that may be overloaded during the crisis.

f. **Securing Hospital Premises**

f1) Access Control

- Lockdown all non-essential entrances and limit access to critical areas of the hospital (emergency department, trauma care, ICUs).
- Set up perimeter security with clear identification and verification of individuals entering the hospital, especially for:
  - Emergency responders
  - Media personnel
  - Family members of victims
- Only allow authorized personnel into triage and critical care zones.

f2) Crowd Management

- Implement crowd control measures to prevent overcrowding in the hospital.
- Designate safe waiting areas for family members, where they can receive updates without disrupting hospital operations.
- Use security personnel to manage panic and maintain order among those seeking information about victims.

g. **Evacuation Protocols**

- Be prepared for partial or full evacuation in case of secondary threats (e.g., bomb threats or structural damage).
- Work with local law enforcement to designate safe evacuation routes and alternative care locations for patients.

h. **Coordination with External Agencies**

h1) Law Enforcement

- Maintain continuous communication with local police and law enforcement agencies to respond to any external threats, such as:
  - Terrorist activity
  - Active shooter situations
  - Public disorder
- Provide real-time updates to the authorities regarding security concerns inside and around the hospital premises.

h2) National Disaster Response Force (NDRF)

- The NDRF is the central agency in India responsible for responding to disasters, including mass casualty events.
- Coordinate with the NDRF and state disaster response teams for:
  - Search and rescue operations
  - Transporting victims
  - Resource allocation (e.g., ambulances, medical supplies)

i. **Managing the Media**

- Designate a media liaison officer within the hospital's ICS to handle media inquiries.
- Establish a media zone outside the hospital to prevent media personnel from interfering with hospital operations.
- Communicate regularly with the media to reduce the spread of misinformation and maintain public trust.

j. **Post-Incident Security and Recovery**

j1) Securing the Hospital After the Event

- After the MCE, ensure that the hospital premises are secure before allowing unrestricted access.
- Perform a security sweep to check for any remaining threats (e.g., suspicious packages or safety hazards).

j2) Psychological Support and Counseling

- Provide mental health support for staff, patients, and families affected by the MCE. Offer counseling services and ensure that psychological first aid is integrated into the hospital's recovery plan.

j3) Debriefing and Review

- Conduct a security debriefing after the event to assess the hospital's security response.
- Review what worked well and where improvements are needed. Update the Mass Casualty Management Plan accordingly.

k. **Training and Drills**

- Regularly conduct disaster response drills, incorporating NDMA guidelines and lessons learned from past events.
- Include all hospital personnel (medical, administrative, security) as well as local authorities and law enforcement in training exercises.

10 COORDINATION WITH EXTERNAL AGENCIES

10.1 Law Enforcement

The local law enforcement authorities primarily the police are mandated to ensure law and order and provide security in all health facilities. The police come in when the patient's safety is in jeopardy or when a crime has been committed within the hospital or its surroundings. This will entail the following:

- **Dealing with Violence and Criminal Activities:** The police come into action in case of violence in the hospital regarding assault, disputes between the patients or their relatives, threatening of hospital staff, etc. Incidents regarding criminal activities, such as drug cases, thefts, and vandalism, are also handled by them.
- **Patient Safety:** When the patients are victims of certain criminal activities, like violence, accident, or even sexual assault, the law enforcement ensures that the legal procedures are enacted and the rights of the patients are preserved.
- **Managing Public Order:** If there are any massive emergencies, protests, or strikes that may affect hospital services, law enforcement provides crowd control and security to keep the operations functional in the facility.

Coordination with Health Facilities:

- **Named Liaison Officer:** Each hospital should designate a named security officer who would liaise with the local police. In that way, in case of an emergency, police can respond without any delays in communication.
- **Establish Clear Protocols:** Management in a hospital should establish clear protocols indicating under what circumstance law enforcement needs to be summoned and how. The protocols should include provisions for reporting crimes, preserving evidence, and also sensitive cases such as domestic abuse.
- **Joint Training and Drills:** To this effect, regular training and exercises in emergency response, including law enforcement, can help the police and hospital staff in how best to handle such incidents as active shooters and other public safety.
- **Legal Compliance:** It is important that hospitals are aligned with the legal framework as relates to the confidentiality of patients and proper documentation of contact made with the police, particularly in cases where there are vulnerable subjects of care present, for instance, minors and victims of domestic violence.

10.2 Fire Department

The fire department has primary responsibilities in areas of fire safety and rescue. Due to hospital's large, complex facility and its vulnerable population, it presents some very unique needs in terms of fire protection and emergency response.

- **Fire Response and Evacuation:** The Fire Department responds for fires and assists in safely evacuating patients, staff, and visitors. This is particularly challenging due to the size of the hospital and the presence of non-ambulatory patients.
- **Fire Safety Audits and Inspections:** Fire departments routinely perform safety audits to ensure that hospitals meet the standards of fire safety through working fire alarms, extinguishers, sprinklers, and marked paths for evacuation.

Coordinating with Healthcare Facilities:

- **Fire Safety Audits:** This will involve periodic audits of the fire safety requirements in close cooperation with the fire department. The purpose was to ensure all local codes on fire safety were adhered to, but it also allowed scrutinising areas for improvement, such as fixing faulty fire alarms or ensuring evacuation routes were clear of impediments.
- **Evacuation mock drills:** Drills with the fire department are essential in familiarising the hospital staff with procedures to be followed during an evacuation of patients, specifically critical care or impaired mobility patients. Such drills tests the ability of the hospital to interface properly with fire personnel during an emergency.
- **Installation of Fire Safety Equipment:** The hospital is supposed to liaise with the fire safety officer to ensure the installation and maintenance of fire alarms, extinguishers, sprinklers, and emergency lighting systems in the whole facility.
- **Fire Alarm Systems Integration:** This integration by hospitals with the local fire department should ensure that in any case of fire emergencies there shall be immediate notification to allow their response without any delay.

(Note: Further details related to fire safety elaborated under chapter 9)

10.3 Emergency Medical Services

Emergency Medical Services, EMS, are the pre- hospital emergency care and are responsible for the conveyance of patients from the site of injury or illness to healthcare facilities.

- **Transportation and Stabilisation of the Patient:** The EMS teams are trained for stabilisation of critically ill/injured patients before their transport to the hospital. It includes the administration of emergency treatment, management of trauma cases, and determination of urgency for transport.
- **Triage and prioritisation:** This would involve the prioritisation of care, such as decisions on who should receive immediate care when dealing with mass casualty incidents, based on the condition's severity as noted and valued by EMS providers.

Coordination with health facilities:

- **Standardisation of the Handover Protocols:** The hospital and EMS should work in tandem when it comes to developing standardised handover practices. This will ensure that when the patient is transferred to the hospital, necessary information about his condition, treatment given to him while on the way to the hospital, and immediate care required by the patient is communicated to the EMS quickly.
- **Seamless Communication:** Hospitals should establish direct communication channels with EMS teams to reduce delays during patient handovers. This could be achieved through dedicated phone lines, or even integrated digital communication platforms.
- **Joint Training Sessions:** Joint simulations and training exercises help both the understanding of others' roles and efficiency of care by EMS and hospital staff. For example, mass-casualty drills involve the EMS and the hospital's emergency department in testing response times and treatment plans.
- **Pre-hospital communication systems:** Hospitals can work with EMS to provide real-time GPS tracking of ambulances and medical telemetry systems that will enable the hospital staff to prepare well in advance of the patient's arrival based on real-time information from the ambulance.

10.4 Other Healthcare Facilities

Cooperation among various other healthcare facilities, such as hospitals, clinics, and specialised care facilities, is very crucial in ensuring that patients receive just the right amount of care.

- **Transferring Patients:** Healthcare facilities sometimes have to transfer patients to other hospitals because of certain treatments that may not be available in that particular place, or for alleviating pressure in an emergency department.
- **Shared Medical Records:** Good coordination ensures that the medical records should smoothly be transferred from one facility to another to maintain continuity in their care.
- **Joint Training Programs:** Joint training sessions can be organised with other healthcare facilities on advanced trauma care and disaster management that will enhance clinical skills and develop better inter-hospital relations.

10.5 Government Regulatory Bodies

The government agencies, such as the Ministry of Health and Family Welfare and the National Disaster Management Authority, ensure that hospitals follow healthcare regulations. Most importantly, in cases of public health emergencies, these agencies often get involved in their operations. It describes the following roles government bodies play in the functioning of the hospitals.

- **Regulatory Oversight:** The government bodies oversee compliance of the hospital with national standards in healthcare related aspects concerning hygiene, patient care, disaster preparedness, and licensing.

- **Public Health Emergencies:** Some outbreaks or even pandemics may require these agencies to provide guidance on implementing quarantine procedures, vaccination drives, or management of mass casualties.
- **Disaster Management:** This could be collaboration in the emergency response to any natural or artificial disasters with regard to patient evacuations and resource management.

Coordinating with Health Facilities:

- **Adherence to Regulations:** For the consideration of compliance with healthcare regulations, standards, facility safety, patient privacy, and medical protocols, the need to work hand in hand with the government agencies arises. To this end, every hospital should have some sort of reporting systems meant for updating regulatory bodies concerning public health concerns, infectious disease outbreaks, or violations of safety measures. As a matter of fact, all disease cases that are notifiable have to be reported to the Ministry of Health.
- **Public Health Campaigns:** This includes cooperation in vaccination campaigns-schools helping government agencies conduct mass vaccinations and availing the respective schools for vaccination centres for COVID-19 or polio vaccinations, amongst others-and promotion of awareness of such drives.
- **Disaster Management Training:** Hospitals can train with institutions such as the National Disaster Management Authority on how to handle disasters such as floods, earthquakes, and bioterrorism threats.

10.6 Procedures for Coordination with External Agencies

The presence of clear-cut procedures regarding coordination in both emergency and routine situations with relevant agencies guarantees that responses, whenever they occur within a healthcare facility, will be prompt, effective, and orderly. These procedures form the basis for handling emergencies in a healthcare facility for the safety of patients and for compliance with the law. The standard procedures that a healthcare facility should follow are highlighted below, with necessary corrections for clarity and detail:

10.6.1 Emergency Coordination

- **Emergency coordination:** These are the actions that are to be taken in the event of an urgent, unanticipated situation requiring intervention of outside agencies like police, fire services, EMS, or public health authorities. Appropriate management of this will help reduce harm and ensure the safety of all patients and staff.

Identify the Incident

Situational awareness and an effective judgment of the need for external agency intervention form the immediate basis of emergency coordination. This would include incidents such as the following:

- **Security threats:** Violence, theft, or other crimes within the hospital-falling assaults on staff or patients.

- **Criminal activity:** Suspected substance abuse cases, domestic violence, and other related criminal activities involving the implication of patients.
- Public health hazards include infectious disease outbreaks, bioterrorism events, and food poisonings that may affect large numbers of people. Fire or hazardous materials include fire outbreaks, chemicals, or other environmental hazards that need the intervention of the fire department.
- **How it is done:** After the identification of the incident, immediately contact the security and management of the healthcare facility. The security personnel would immediately implement all steps needed to ensure the safety of the staff and patients, while the management would implement contacting external agencies.

(ii) Contact Relevant Agency

- **Law Enforcement:** If the incident involves a criminal threat or there is a security breach.
- **Emergency Medical Services:** In case of an emergency requiring further transportation or medical attention. Fire Department: When there is fire, spillage of hazardous material, or detection of smoke. Public Health Authorities: Diseases outbreaks, food-borne illnesses, or biohazard dangers.
- **Procedure:** Calls must be placed using the provided emergency contact numbers, made available to all personnel needing it for direct communication with law enforcement, fire services, or EMS. The call should clearly and concisely deliver all the required information, including location, nature of emergency, and number of persons involved.

(iii) Documentation

Accurate and detailed documentation is necessary for legal, medical, and administrative purposes. This allows one to refer back to what occurred after the crisis has been dealt with and how it could be dealt with better next time.

- Document the following:
    - Date and time of incident.
    - Type of incident: fire, patient violence, criminal act
    - Any communication with external agencies: who was contacted and what was discussed.
    - Follow-up activities or continuing actions such as police investigations, public health inspections initiated by hospital personnel and other external agencies.
    - Record-keeping allows transparency and accountability to avoid any legal entanglement.

(iv) Patient Confidentiality

Healthcare organisations are responsible for national privacy laws about the release of patient information to agencies. Most often in India, it means following the principles of patient confidentiality under the Indian Medical Council Act and related legal frameworks.

- **Limit disclosure to what is necessary:** No information concerning a patient should be disclosed unless it is necessary to resolve the incident itself. Examples include law enforcement requesting information about a patient that may be part of a criminal investigation, or the infectious disease information that may be shared with public health authorities.
- **Obtain appropriate permission:** If there is any doubt that permission should be obtained from the patient or representative before disclosing sensitive information, disclosure should not be made - except under compulsion of law, as would be requirements in interests of national security and under court order.

Ensure that there is compliance with laws related to privacy, without any unwarranted disclosure of patient information.

10.6.2 Routine Coordination

In addition to emergency responses, healthcare facilities must engage in routine coordination with external agencies to ensure preparedness and build effective working relationships.

(i) Regular Communication

Maintaining ongoing communication with external agencies (e.g., law enforcement, fire departments, and public health authorities) helps the hospital stay informed of any relevant updates to procedures, legal requirements, or threats.

- **Procedure:**
  - Schedule periodic meetings with representatives from local law enforcement, EMS, fire services, and public health bodies. This could be on a quarterly or bi-annual basis to review current protocols and address any changes or new developments.
  - Establish liaisons in each department to serve as points of contact for external agencies. These liaisons can facilitate communication and ensure smooth coordination during emergencies.

Regular communication also builds trust and familiarity between agencies, which improves response times and efficiency during actual crises.

(ii) Joint Training Sessions

To be effective in emergency situations, hospital staff and external agencies must be trained together. This ensures that both teams understand each other's procedures and can act in a coordinated manner when a crisis occurs.

- **Procedure:**
  - Conduct joint drills simulating various types of emergencies (e.g., active shooter drills, mass casualty incidents, fire evacuations, infectious disease outbreaks) that involve both hospital staff and external agencies.
  - Include EMS, law enforcement, fire department, and public health officials in these training sessions. This will enhance coordination and ensure that everyone is on the same page when it comes to patient safety, communication, and legal compliance.

These training sessions should be reviewed and refreshed annually to ensure they stay relevant and up to date with current best practices.

(iii) Review and Update Protocols

Emergency coordination protocols must be reviewed regularly to ensure that they are current and comprehensive. This includes revising procedures based on lessons learned from previous incidents or changes in regulations and technology.

- **Procedure:**
  - **Annual review:** Healthcare management should review all emergency coordination protocols on an annual basis, updating any procedures that are outdated or inefficient.
  - **Post-incident review:** After any major incident that involved external agencies, conduct a debriefing session to evaluate what went well and identify areas for improvement. This will help refine protocols and enhance preparedness for future incidents.

By regularly updating protocols, healthcare facilities ensure that their response systems remain effective and legally compliant, helping to improve overall safety.

10.6.3 Reporting and Documentation

Proper reporting and documentation are essential for maintaining transparency, accountability, and legal compliance when coordinating with external agencies. These practices ensure that all actions taken during and after an incident are clearly recorded and can be reviewed for future improvements.

10.6.4 Incident Reports

After each incident that requires external agency involvement, it is critical to complete a detailed incident report.

Purpose: Incident reports help document what happened, the steps taken, and the outcomes. These reports are used for internal review, improving protocols, and providing necessary information for legal or insurance purposes.

- **Key Components of an Incident Report:**
  - **Date and time of the incident:** Record when the incident occurred and when it was reported.
  - **Type of incident:** Specify the nature of the emergency (e.g., fire, security breach, patient violence).
  - **External agencies involved:** List the agencies that were contacted, such as law enforcement, EMS, or fire services.
  - **Actions taken:** Document the actions taken by hospital staff before and after contacting external agencies.
  - **Communication details:** Note all communications with external agencies, including the names of the people contacted and the information shared.

- **Outcome:** Summarize the result of the incident, including whether the situation was resolved, if patients were transferred, or if further action is required (e.g., police investigations or public health interventions).
- **Procedure:** Incident reports should be completed as soon as possible after the situation is resolved to ensure accuracy. They should be reviewed by hospital management and stored securely for future reference.

10.7 Records Maintenance

Maintaining detailed and organized records of all communications and actions related to external agency coordination is crucial for legal compliance, transparency, and internal auditing.

- **Purpose:** These records serve as a reference for future emergencies, allow for post-incident evaluations, and help identify areas for improvement in hospital protocols.

Key Elements to Record:

- **All communications with external agencies:** This includes emails, phone calls, radio transmissions, and any other form of communication. Details such as the date, time, and nature of the conversation should be recorded.
- **Documentation of actions:** Any actions taken by hospital staff, external agencies, or both should be documented thoroughly, ensuring a clear timeline of events.
- **Outcomes and follow-ups:** Keep records of the outcomes of incidents and any follow-up actions taken with external agencies (e.g., continued police investigations, public health follow-ups).
- **Procedure:** Records should be maintained in a secure system accessible only to authorized personnel. This helps ensure data integrity and confidentiality while making it easy to retrieve information when needed.

10.8 Confidentiality and Legal Compliance

Healthcare facilities are bound by strict patient confidentiality laws when sharing patient information with external agencies. Ensuring legal compliance when sharing sensitive data is critical to protecting patient privacy and adhering to national regulations

10.8.1 Patient Confidentiality

Confidentiality in healthcare is the practice of protecting patient information from unauthorized access. This includes medical records, personal identification, and details related to their treatment.

- **Legal Frameworks:** While HIPAA (Health Insurance Portability and Accountability Act) is specific to the U.S., in India, healthcare confidentiality is governed by:
- **Indian Medical Council Act, 1956:** This outlines the ethical duties of doctors to maintain confidentiality.
- **Information Technology Act, 2000:** This act includes provisions on the protection of sensitive personal data, including healthcare records.

- **Procedure:**
  - **Minimize data sharing:** Only share the minimum necessary patient information when coordinating with external agencies. For instance, law enforcement may need to know certain facts about a patient's involvement in a criminal case, but full medical records should not be disclosed unless legally required.
  - **Obtain consent when possible:** Always seek patient consent before sharing their information with external agencies, unless an exception applies (e.g., public safety threats, court orders, or cases where patient capacity is compromised).
  - **Confidential reporting systems:** Develop secure systems for sharing patient data, ensuring that only authorized personnel can access it, and that all legal requirements are adhered to.

10.8.2 Legal Compliance

Healthcare facilities must ensure compliance with all relevant laws and regulations when sharing information or coordinating with external agencies.

- **Procedure:**
  - **Know the legal requirements:** Healthcare staff should be trained in national and local laws governing patient confidentiality and information sharing. This includes understanding the limits of information that can be shared with law enforcement, EMS, or public health authorities without violating privacy laws.
  - **Documentation of consent:** If patient information is shared with an external agency, the hospital must document whether consent was obtained or if legal exceptions applied.
  - **Regular audits:** Conduct regular audits of all data-sharing practices to ensure compliance with national privacy laws and to identify areas for improvement in information security.

10.8.3 Review and Monitoring

Continuous review and monitoring of the Standard Operating Procedures (SOPs) are essential to ensure they remain effective, relevant, and up-to-date. Healthcare facilities operate in dynamic environments where protocols may need to evolve based on new regulations, technologies, and lessons learned from past incidents.

a) Annual Review

SOPs should be reviewed regularly, with a minimum frequency of every 12 months, to assess their effectiveness and make necessary updates.

- **Purpose:** An annual review helps identify gaps, inefficiencies, or outdated information in the SOPs and ensures that the procedures are aligned with current best practices and legal requirements.
- **Procedure**:
  - **Conduct an internal audit:** Appoint a review committee consisting of healthcare management, administrative staff, medical personnel, and external agency liaisons to conduct a thorough audit of the SOPs.

- **Evaluate past incidents:** Analyze the facility's incident reports and records from the previous year. Identify patterns, response times, and any coordination issues that arose when working with external agencies.
- **Incorporate lessons learned:** Based on the findings from past incidents, revise procedures to address any weaknesses or challenges. This could include updating communication protocols, improving response strategies, or enhancing staff training.
- **Regulatory updates:** Ensure that the SOP reflects any changes in national or local healthcare regulations, patient confidentiality laws, or requirements set by external agencies.
- **Feedback from staff and external agencies:** Gather input from hospital staff and external agencies (e.g., law enforcement, EMS, fire department) to identify areas for improvement.

b) Monitoring Effectiveness

Monitoring the effectiveness of the SOP involves regular oversight to ensure that the procedures are being followed correctly and that they are producing the desired outcomes.

- **Procedure:**
  - **Real-time monitoring:** Appoint a monitoring team to oversee the implementation of SOPs during emergencies or drills. This team should track response times, communication flow, and coordination with external agencies.
  - **Post-incident evaluations:** After every major incident, conduct a debriefing session to assess how well the SOPs were followed. Identify any deviations from the SOPs and their impact on the outcome of the incident.
  - **Performance metrics:** Develop performance metrics (e.g., response times, patient outcomes, coordination efficiency) to measure the success of the SOP in real-time situations.
  - **Compliance audits:** Periodic compliance audits should be conducted to ensure that staff is following the SOPs properly. This includes checking that documentation is complete, protocols are adhered to, and communication is handled effectively.

c) Updates as Needed

If any significant gaps or issues are identified during the review or monitoring process, immediate updates to the SOP should be made, rather than waiting for the annual review.

- **Procedure:**
  - **Emergency revisions:** In case of a major incident or regulatory change, the SOP should be revised promptly to address the new requirements.
  - **Communicate changes:** Ensure that any updates to the SOP are communicated to all relevant staff through formal training sessions or internal announcements.
  - **Re-training:** If significant changes are made to the SOP, staff should undergo refresher training to ensure they understand and can implement the updated procedures effectively.

ANNEXURE-1

(CYBER- SECURITY)

1. Specific Challenges Faced by Hospitals

Hospitals face unique challenges when implementing cyber- security measures, largely due to the complexity of their systems, regulatory requirements, and the critical need for operational continuity.

1. **Legacy Systems**
   - Many hospitals operate with legacy systems and outdated medical devices that were not originally designed with cyber security in mind. These older systems often lack the ability to support modern security protocols, making them vulnerable to attacks.
   - Replacing or upgrading legacy systems can be costly and disruptive to healthcare services, which complicates efforts to modernize hospital IT infrastructures.
   - Examples include older versions of hospital management software, diagnostic equipment with obsolete firmware, and non-networked devices that cannot be easily secured.
2. **High-Value Targets for Cybercriminals**
   - Hospitals are considered high-value targets due to the sensitive nature of the data they handle and the critical services they provide. Cybercriminals exploit this dependency to launch ransomware attacks, knowing that hospitals may feel compelled to pay ransom to restore services quickly.
   - Additionally, hospitals are rich sources of personal, financial, and medical data, which can be sold on the dark web or used in identity theft schemes.
   - The high volume of data handled by hospitals, coupled with the urgency of patient care, creates numerous attack surfaces for cybercriminals.
3. **Compliance with Multiple Regulations**
   - Hospitals must adhere to stringent data protection laws, such as the DPDP Act and the Information Technology Act in India, as well as health-specific guidelines like the National Digital Health Mission (NDHM). Balancing regulatory compliance with operational needs can be complex.
   - Fines and penalties for non-compliance can add to the financial burden of a hospital following a data breach.
4. **Growing Threat Landscape**
   - As hospitals increasingly adopt digital tools and interconnected medical devices (Internet of Medical Things, IoMT), the potential entry points for cyberattacks grow. IoMT devices are often minimally secured, expanding the attack surface.
   - The sophistication of cyberattacks has also evolved, with attackers using advanced techniques such as spear phishing, social engineering, and zero-day vulnerabilities to breach hospital systems.

2. Components of Network Security

Several key components work together to secure hospital networks. These include:

- **Firewalls:** Firewalls act as the first line of defense by filtering incoming and outgoing traffic based on predefined security rules. They create a barrier between the hospital's internal network and external threats, blocking potentially harmful traffic. Types of firewalls include network-based firewalls that protect the entire hospital network and host-based firewalls that provide protection at the individual device level, such as laptops and workstations. Firewalls can be configured to block suspicious IP addresses, restrict access to certain websites, and allow only authorized traffic into sensitive areas of the network.
- **Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS):** IDS monitor network traffic for malicious activities or policy violations, alerting administrators when such activities are detected. However, IDS only provides alerts and does not take any automatic action. IPS take a proactive role by not only detecting threats but also automatically responding to them. An IPS can block suspicious traffic or terminate malicious processes before they cause harm. Both IDS and IPS are essential for early detection and mitigation of threats in hospital networks, which often contain sensitive data and connected medical devices.
- **Virtual Private Networks (VPNs):** VPNs create a secure, encrypted connection between a user's device and the hospital's internal network, ensuring that data transmitted over the connection remains private and protected. VPNs are particularly useful for allowing remote healthcare professionals, such as telemedicine providers or traveling doctors, to securely access hospital systems without exposing data to the public internet.
- **Encryption:** Encryption ensures that sensitive data, whether stored or in transit, is unreadable to unauthorized users. Hospitals use encryption to protect patient records, financial information, and communications between healthcare providers. End-to-end encryption can be employed to secure sensitive medical data during transmission, making it critical for preventing data breaches when accessing systems remotely or sharing information across different departments.

3. The Role of Virtual Private Networks (VPNs) and Encryption

VPNs and encryption are two critical components of securing hospital networks:

- **VPNs:** A VPN allows secure remote access to the hospital's internal network by encrypting the data that passes between the user's device and the hospital's servers. This is especially important for healthcare workers accessing hospital systems remotely, as well as for telemedicine services. By tunneling internet traffic through secure servers, VPNs prevent external parties from intercepting sensitive data, such as patient information or treatment plans. In a hospital setting, VPNs are used to securely connect different branches, clinics, or external partners to the central hospital network.
- **Encryption:**
    - **At-rest encryption:** Ensures that stored data (such as patient records in databases) is secure and cannot be read without the proper encryption key. This protects against data breaches even if physical access to the servers is compromised.

- **In-transit encryption:** Protects data moving across networks, such as when sharing patient information between departments, ensuring that it cannot be intercepted by unauthorized parties.

4. Data Protection during Transmission

Data transmission in hospitals happens between internal systems, external partners (such as insurance companies), and between departments. Protecting data during transmission is critical to ensuring that sensitive information is not intercepted or altered as it moves across networks. Strategies for protecting data during transmission include:

- **End-to-End Encryption:** Encrypting data during transmission ensures that even if it is intercepted, it cannot be read or modified by unauthorized individuals. This applies to communications between doctors, departments, and external parties, such as sharing test results or medical reports.
- **Secure Protocols:** Hospitals should use secure communication protocols, such as HTTPS (Hypertext Transfer Protocol Secure) or SFTP (Secure File Transfer Protocol), to protect data in transit. These protocols ensure that data exchanged between systems remains encrypted and secure.
- **Virtual Private Networks (VPNs):** VPNs should be used to secure data transmitted between remote locations or offsite workers, as they create encrypted tunnels that protect the data from external threats.

5. Training Frequency and Methods

Cyber- security training should be an ongoing process rather than a one-time event. Frequent, engaging training sessions help reinforce cyber- security best practices and keep hospital staff updated on emerging threats.

- **Training Frequency:**
  - **Initial Onboarding:** All new employees should receive comprehensive cyber-security training during onboarding, covering general awareness and role-specific content.
  - **Annual Training:** Hospitals should conduct mandatory refresher courses for all staff at least once a year to reinforce key principles and introduce updates in cyber- security practices.
  - **Periodic Updates:** Short, periodic training sessions or reminders can be provided to address emerging threats, such as new phishing tactics or ransomware risks.
- **Training Methods:**
  - **Simulations:** Conducting phishing simulations or mock cyberattacks can help employees identify potential threats in real-time and practice the appropriate responses. These simulations also allow hospitals to assess their staff's readiness to handle cyber- security incidents.
  - **Workshops and Webinars:** Interactive workshops and webinars allow staff to engage with cyber- security experts, ask questions, and gain hands-on experience in recognizing and mitigating threats.
  - **E-learning Platforms:** Hospitals can use online courses to deliver flexible, role-specific cyber- security training. E-learning platforms also allow staff to learn at their own pace and track their progress.

6. 8.5.5 Creating a Culture of Cyber- security Awareness in Hospitals

Establishing a culture of cyber- security awareness requires more than just training—it involves integrating cyber- security into everyday practices and fostering a collective responsibility for protecting hospital data.

- **Leadership Involvement:** Hospital leadership should actively participate in and promote cyber- security awareness efforts. When senior management emphasizes the importance of cyber- security, it sends a clear message that protecting sensitive data is a priority for everyone.
- **Clear Communication:** Hospitals should create open channels of communication between IT teams and staff, allowing employees to report potential threats, ask questions, and receive guidance without fear of reprimand. IT departments should also regularly update staff on new threats or changes in security policies.
- **On-going Engagement:** Cyber- security awareness should be a continual focus in the hospital's operations. This can be achieved through:
  - Regular cyber- security newsletters or updates that keep staff informed of new threats and best practices.
  - Posters or reminders in high-traffic areas to reinforce cyber- security tips, such as creating strong passwords or reporting suspicious emails.
  - Encouraging a "see something, say something" approach, where employees feel empowered to report suspicious activities or vulnerabilities.
- **Accountability and Recognition:** Holding staff accountable for following cyber- security best practices, while also recognizing those who excel in maintaining security, can create a positive cyber- security culture. Hospitals may implement reward programs for employees who consistently demonstrate cyber- security vigilance.

6. Role of the IT Department in Hospital Cyber- security

The IT department plays a central role in hospital cyber- security by managing the technical infrastructure, implementing security measures, and responding to cyber threats. Hospitals rely on IT professionals to protect sensitive data, secure network systems, and ensure the smooth operation of clinical and administrative functions. Key responsibilities of the IT department in hospital cyber- security include:

- **Implementing security controls:** The IT department is responsible for deploying and managing cyber- security technologies such as firewalls, intrusion detection systems (IDS), encryption, and anti-malware tools to protect hospital systems from cyberattacks.
- **Maintaining network security:** IT teams manage hospital networks, ensuring that connections are secure and protected against unauthorized access, data breaches, and potential vulnerabilities.
- **Incident response:** In the event of a cyber- security breach or attack, the IT department leads the response efforts by identifying, containing, and mitigating the threat. This includes restoring systems, safeguarding data, and preventing further damage.
- **Compliance management:** IT teams help ensure that hospital systems comply with cyber- security regulations and standards, such as the Digital Personal Data Protection (DPDP) Act, IT Act, and frameworks like ISO 27001 and COBIT.

The role of the IT department is proactive and ongoing, as they must constantly monitor systems, update security protocols, and prepare for potential cyber threats.

7. Understanding Different Types of Cyber- security Attacks and IT Responses

Cyber- security threats evolve constantly, and both healthcare and IT teams must understand the various types of attacks that can target hospitals. Common attacks include:

- **Phishing and social engineering:** IT teams often detect phishing attempts and work to block malicious emails before they reach hospital staff. They also educate staff on how to recognize phishing attacks and avoid falling victim.
- **Ransom ware:** In the event of a ransom ware attack, IT teams will work to isolate affected systems, prevent the spread of the malware, and begin recovery procedures using backups. Hospitals are frequent targets for ransom ware due to the critical nature of their services.
- **Insider threats:** Insider threats involve malicious or accidental actions by hospital staff. IT teams monitor for unusual activity, such as unauthorized data access, and work with HR and legal departments to address potential insider threats.
- **Advanced persistent threats (APTs):** APTs are sophisticated attacks where cybercriminals gain long-term access to a network to steal sensitive data. IT teams use advanced monitoring tools and network segmentation to detect and respond to such threats before significant damage is done.



Association of Healthcare Providers (India)
404, Ashoka Estate, Barakhamba Road, Delhi, 110001
011 43095694 | contact@ahpi.in | www.ahpi.in