Laguna Honda Hospital and Rehabilitation Center

Security Management Plan 2017-2018

REFERENCES

California Code of Regulations, Title 8, Sections 8 CCR 3203 *et seq.*
California Code of Regulations, Title 22, Sections 22 CCR 70738
Health & Safety Code, Section 1257.1, 1257.8, 1257.7

I.   PROGRAM OBJECTIVES, INTENT and CORE VALUES

Laguna Honda Hospital and Rehabilitation Center is committed to providing a safe, secure, accessible, and effective environment of care, consistent with its mission, scope of services and applicable governmental mandate. This commitment includes the provision of a physical environment that minimizes the risk of harm to patients/residents, served, staff, volunteers, contractors, and visitors.

It is the overall intent of this plan is to establish the framework, organization, and processes for the development, implementation, maintenance, and continuous improvement of a comprehensive Security Management Program. This program is designed to provide protection through appropriate staffing, security technology, and environmental controls.

The objectives of the Security Management program include:
- Continuous review of physical conditions, processes, operations, and applicable statistical data to anticipate, discern, assess, and control security risks, and vulnerabilities
- Ensure timely and effective response to security emergencies
- Ensure effective responses to service requests
- Report and investigate security related incidents
- Promote security awareness and education
- Enforce various hospital rules and policies
- Establish and implement critical program elements that safeguard people, equipment, supplies, medications, and control traffic in and around the hospital and the outlying buildings.

II.   SCOPE and APPLICATION

The Security Management Plan comprises standards applicable to addressing and facilitating the protection, welfare, safety, and security of the environment. Included is a full range of protective services for persons, property, and assets at the hospital and outlying medical offices. The Security Management Plan requires compliance with all policies and procedures. The management plan calls for best in class customer service for patients/residents, visitors, volunteers, contractors, and staff as well as the protection of property and assets.

The scope of the plan addresses all program elements required to provide a safe and secure environment. Key aspects include:

- Program planning, design, and implementation
- The measurement of outcomes and performance improvement
- Risk identification, analysis, and control
- Reporting and investigating of incidents, accidents, and failures
- Security Awareness, education, and training
- Emergency response
- Addressing legal and criminal matters
- Use and maintenance of equipment, locks, physical barriers, CCTV systems, alarms, etc.
- Security of medications;
- Traffic control
- Security of sensitive areas

III.   AUTHORITY

The SF Health Network provides the program's vision, leadership, and support. The Director of Health appoints a Director of Security who is responsible for the oversight of security program development, and implementation. The Director of Security reports to the Director of Health, and provides security consultation to the LHH Executive Administrator.

IV.   RISK ASSESSMENT

Security risks, vulnerabilities, and sensitive areas are identified and assessed through ongoing facility-wide processes that are coordinated by the Director of Quality Management, Chief Operations Officer, the Director of Security, and the contract security provider. These processes are designed to proactively evaluate facility grounds, periphery, behaviors, statistics, and physical systems. Considerations include:

- Routine Safety/Environmental of Care Rounds
- Root Cause Analysis of significant events
- Failure Mode and Effects Analysis (FMEA)
- Sentinel Event Alerts
- Security Patrols
- Unusual Occurrence Reports- Review of pertinent data/information, incident reports, evaluations and risk assessments
- Community crime statistical data or CAPRISK Reports
- Facility crime, incident and property loss statistics (UO and SFSD Crime stats)- including workplace violence statistics
- Customer and benchmarking surveys
- At Risk patients/residents (such as clinically indicated restraints, medical holds, and stand-by services)
- Hours of operation
- Employee, resident and visitor identification
- Hospital and Rehabilitation Center operations and processes

The profile of potential risks results in an integrated approach to risk control and management. Identified "Sensitive Areas" include the PHI Areas, Administrative Offices, Human Resources, Pharmacy, Nutritional Services, and Psychiatry.

V.   PROGRAM ORGANIZATION AND RESPONSIBILITIES

The Director of Security is responsible for the quality oversight of the security program. The Director of Security in partnership with the contract security provider, San Francisco Sheriff's Department, SFSD is responsible for the overall management of the security program. This includes the program design, implementation, identification, control of risks, staff education, and training, and consultation.

The Director of Security manages the security program across all divisions of DPH and coordinating the implementation of the MOU with the San Francisco Sheriff's Department, ensuring that DPH staff are trained, follow established policies and procedures, comply with regulatory requirements, overseeing and maintain security technology and equipment, tracking, analyzing, and reporting on security incidents, and recommending improvements, reviewing and sharing building plans for new construction and renovations for security issues such as accessibility, alarms, lighting and landscaping; ensuring that annual security risk assessments are completed, and ensuring that the appropriate resources are available to accomplish the objectives and goals of the security management plan. The Director of Security reports to the LHH Campus Safety and Security Committee (CSS), and Executive Committee about the implementation of new procedures and operations, as well as installation of new systems.

The SFSD Unit Commander manages the security, public safety, and law enforcement services at sites under DPH control, including providing security and law enforcement personnel, management of security and law enforcement operations, and compiling information from incident reports to form the quarterly reports that are submitted to the LHH, CSS, and Executive Committee. The Unit Commander assures that security and law enforcement staff receive hospital related training, participate in appropriate violence prevention, safety and security, and threat management committees; and assures that SFSD staff, assigned to LHH follow hospital security operation procedures.

The Director of Security Services and the SFSD Unit Commander will collaboratively establish and maintain communication and mutual ownership for outcomes, identification and troubleshooting of emergent safety concerns, compliance with hospital regulatory standards and requirements; service level agreements, resources and performance metrics; clearly defined accountabilities and responsibilities; strategic and joint addressing of long-term and underlying safety conditions and solutions; customer service and professionalism of personnel providing security and law enforcement; and creating a culture of safety and security.

The LHH Safety and Security (CSS) Committee is comprised of clinical, administrative, operations support services, and labor representatives who ensures that the security management program is aligned with the core values and goals of the organization by providing direction, setting strategic goals, determining priority and assessing the need for change. The LHH CSS Committee is the central hub of the Information Collection and Evaluation System and acts as a clearinghouse for action items, recommendations, and ensuring that risks are controlled in a timely fashion. The committee also ensures coordination, communication and integration of performance improvement, strategic planning and injury prevention activities in committee activities.

In the context of security management, the LHH CSS Committee is designed to:
- Develop strategic goals and annual performance targets, relative to Security and the Safety Program.
- Carry out analysis and seek timely, effective, and sustainable resolution to security related issues
- Prioritize goals and resources

Department managers are responsible for the provision of a safe and secure work environment for staff through full implementation of established LHH CSS Committee programs. This includes the identification of security risks, staff education, developing and implementing department specific security policies and procedures, incident reporting, and the protection of patients and their belongings.

Employees are responsible for following security policies and practices about personal protection and reporting of security incidents, risks and threats. Employees include contract employees, volunteers, students, registry personnel and anyone working under the facility's auspices.

VI.   PROGRAM IMPLEMENTATION AND PROCESSES

Successful implementation of the Security Management Plan involves the incorporation of the principles of the plan into the culture and operations of the organization. Implementation of the security program is the responsibility of the Director of Security, and SFSD Unit Commander. The performance is monitored quarterly by the Safety Committee and the Executive Committee. They include:

1. The designation of a person to be responsible for program development and oversight. The Health Director has designated the Director of Security as the person responsible for the quality oversight of the security program's development, implementation and monitoring.

2. The Security Services Department and the San Francisco Sheriff's Department conduct investigations and completes written reports about security incidents involving patients, staff, visitors, volunteers, and property. Investigations are documented and reviewed by the SFSD Unit Commander and the DPH Director of Security. Corrective actions are developed and implemented to mitigate risks. The Director of Security in collaboration with the SFSD Unit Commander ensures that incident reports are distributed to the appropriate departments (i.e. Quality, Risk Management, etc.) Significant events are reported to the Executive Administrator, and the Administrator-on-Duty and to the Director of Workplace Safety and Emergency Management.

3. Security will ensure that employees, vendors, and contractors wear personnel identification badges to facilitate the creation of a safe and secure environment. Badges are issued to all employees, consultant physicians, volunteers, and vendors.

4. Access to the hospital's perimeter and buildings is maintained by a lock down of unoccupied areas, routine checks on all perimeter doors, and the securing of individual departments after normal business hours. The contract security provider ensures that access to the facility is restricted by confirming unauthorized personnel and escorting them off the premises.

5. *Security controls access to and egress from security sensitive areas by means of direct observation, locks and other physical barriers, signage, alarm systems and access control systems.*

6. The contract security provider conducts regular foot and vehicular patrols to identify potential security risks and assess the status of physical conditions within the buildings and on the hospital grounds. Regular patrols and security checks of stairwells, campus interior and exterior, and parking areas are conducted to deter theft, vandalism and other criminal activity. Security and Law Enforcement presence includes foot patrols, vehicle patrols and recording of CCTV cameras in the Security Operations Center and maintaining fixed positions.

7. The Director of Security is actively involved in a multidisciplinary, hospital wide Threat Management Team, and provides both investigative and protective services. The Director of Security in collaboration with the SFSD work closely with Administration, Human Resources, the Department of Public Health, and other law enforcement agencies on matters concerning criminal cases, threat management investigations, and other non-criminal cases.

8. The Security Operations Center monitor all alarms, radio, and security telephone transmissions to ensure that the appropriate actions are initiated and communicated.

9. The Security Services Department, and SFSD maintains records of all incident reports, service calls and crime statistics. Incident reports that involve safety, patients, and environmental issues will be forwarded to the Safety Manager and the Risk Manager.

10. The Security and Facilities Department maintains and coordinates the card access program. The requestor submits an Access Card Request form signed by the requestor's manager. The Access Card Request form is reviewed by the Facilities Department to determine the need for the requestor to have card access. Approved Card Requests are processed by Facilities. Records of all issued access cards are maintained with Human Resources and Facilities.

11. The SFSD provides emergency response for the following:

- Code Blue – Upon notification, to providing crowd control as needed
- Code Red – Upon notification, respond to the alarm point of origin to assist in implementing initial fire plan, provide assistance to local fire department and Facilities.
- Internal / external disasters - providing staff to control access to the facility and provide assistance to/from local emergency response agencies
- Code Green - deploy security personnel to designated locations to establish a perimeter and begin the search for the missing patient.
- Managing situations involving media or VIPs by providing assistance to the Information Office and/or Administration and safeguarding info on any VIP on premises.
- Lockdown Procedure - Heightening existing security measures as needed during civil unrest, disturbances, or acts of terrorism.
- Security also provides emergency assistance to medical/clinical staff, including but not limited to stand-by services, patient restraints, searching for missing persons, crowd control, response to duress alarms, etc.

12. All new employees, at the time of hire, will attend a New Employee Orientation Program. All employees will receive basic information related to the Security Department and its Security Management Plan. During the security portion of the orientation, employees will receive information about the following:

- A description of the Security Department
- Security services provided
- Prudent security practices
- ID Policy
- Unusual Occurrence (UO) System
- Stairwell Security
- Reporting a security incidents or suspicious activity
- Security locations and phone numbers, etc.

13. Additional training will be administered as needed to assure competency in federal, state, local laws, and regulations: Crisis Prevention and Intervention, Management of Aggressive Behavior and Threat and Workplace Violence response.

14. The SFSD Unit Commander will verify that each SFSD employee assigned to Laguna Honda Hospital and Rehabilitation Center complete the required New Employee Orientation Training, six week Healthcare Security Training, and core competencies with respect to security emergencies.

15. Documentation will be retained by the Department of Education and Training and/or the SFSD Training Coordinator. Security refresher in-services will be based on the assessment of the department's need, change in roles or regulatory requirements and/or findings of the Safety and Emergency Management Committees.

VII.   PROGRAM EFFECTIVENESS

Through the LHH Safety and Security Committee, the effectiveness of the security program is monitored and assessed on an ongoing basis. Identified risks are used to develop performance measures to create a safe and secure environment for staff, patients and visitors to the hospital. Performance is reported to the LHH Safety and Security, and Executive Committee on a quarterly basis. Recommendations are made as needed to facilitate improvements in performance. Action plans are developed and implemented as needed to improve performance.

VIII.   PERFORMANCE

The hospital has developed and implemented a systematic, department-wide approach for performance improvement. It is intended to assist the hospital in developing and maintaining improvement programs that are meaningful, realistic, and adjustable based upon relevant data and customer feedback. The standards and metrics by which the performance of this plan will be measured are based on hospital and department experiences, 2015 Security Risk Assessment, exercise evaluation results, observed work practices, customer expectations/satisfaction, and/or LHH Safety and Security, and Executive Committee recommendations.

During 2017-2018, the measures that will be collected, tracked and analyzed by the Safety, and Executive Committee on a quarterly basis include:

Performance Metric #1 – Code Green, "At Risk" Patient Alert Response Incidents and Drills:

During actual Code Green incidents/drills, the effectiveness of the contract security provider will be measured to determine their response in the following areas:

- Initial Perimeter and Search
- Notification of SFPD, BART, and MUNI
- Documentation of Search Activity
- Locate/Not Located Procedure

1. The contract security provider will be measured on their ability to effectively respond i.e. initial perimeter search, and notification of SFPD, BART, and MUNI as applicable, and document the search activity:

   Response-rate Threshold – 80%
   Response-rate Target – 90%
   Response-rate Stretch – 100%

2. The contract security provider will be measured on its ability to locate and return an "At Risk" resident/patient, and when they are not located, follow the Not Located Procedure.

   Locate/Return-rate Threshold –90%
   Locate/Return-rate Target – 98%
   Locate/Return-rate Stretch – 100

Performance Metric#2 – Customer Satisfaction:

In accordance with the scope of the security management plan, the management plan calls for best in class customer service for patients, visitors, volunteers, contracts and staff. On a quarterly basis, a sample size of 100 customers, consisting of patients/residents, visitors, volunteers, contractors, employees, and consultant physicians that had a recent contact with Security Services, will be surveyed on their experience.

Customers will respond as either, Very Satisfied, Satisfied, Somewhat Satisfied, Dissatisfied, and Very Dissatisfied in the following areas:

- Responsive
- Treated with dignity and respect
- Courteous
- Effective
- Overall Experience

Threshold - 80% Somewhat Satisfied
Target - 90% Satisfied
Stretch – 98% Very Satisfied

Performance Metric#3 – Electronic Security System Functionality:

On a monthly basis the Security Operations Center will inspect the electronic security system for functionality. The Facilities Department will monitor all service call/work-orders to ensure timely response. The Security Director and SFSD Unit Commander will develop a plan to mitigate risk, resulting from system malfunctions. The action plan will be documented in EOC Security Report.

The monthly target is for 100% of the system to be inspected, and will be 98% functional.

Significant Event Reporting – The following events will be reported to the Campus Safety and Security, and the Executive Committee quarterly, which will be included in the EOC- Security Report.
- DPH and SFSD, MOU Performance Metrics
- Serious Incident Crime Stats
- Use of Force Statistics

IX.   ANNUAL PROGRAM EVALUATION ANNUAL PROGRAM EVALUATION

On an annual basis, the security management program is evaluated relative to its objectives, scope, effectiveness and performance. This evaluation process is coordinated through the Director of Security, in conjunction with the contract security provider, LHH Safety and Security Committee, and the Executive Committee.   The continued appropriateness and relevance of program objectives are assessed, as well as whether or not these objectives were met. The scope is evaluated to determine continued applicability. The year is reviewed retrospectively to determine the extent to which the program was effective in meeting the needs of the hospital, the residents and staff. The performance results are assessed as an indicator of ongoing performance improvement. Results of this evaluation process will form the basis for strategic goal setting, planning, and verifying the continued applicability of program objectives.