

PRISMA HEALTH RICHLAND

SECURITY MANAGEMENT PLAN 2020

I. SCOPE

The Security Management Plan describes the procedures for providing security for people, equipment and other materials through security assessments and management for Prisma Health Richland. Security protects individuals and property against harm or loss. This includes workplace violence, theft, infant abduction, and restricted access to medications or other sensitive areas. Patients, visitors or staff members at the facility cause security incidents and they are often intentional.

Prisma Health Richland is committed to improving the physical, emotional, and spiritual health of all individuals and communities we serve; to providing care with excellence and compassion and to work with others who share our fundamental commitment to improving the human condition.

This program is applied to the Prisma Health Richland and off-site facilities.

II. FUNDAMENTALS

- A. A visible security presence in the hospital environment helps reduce crime and increase feelings of security for patients, visitors, and team members.
- B. The assessment of risks to identify potential problems is central to reducing crime, injury, and other incidents.
- C. Analysis of security incidents provides information to predict and prevent crime, injury, and other incidents.
- D. Training of hospital team members is crucial to ensuring their performance during a security emergency. Team members are also trained to recognize and report either potential or actual incidents to ensure a timely response.
- E. Team members in sensitive areas are trained to implement protective measures designed for those areas and what their responsibilities are to assist in the protection of patients, visitors, team members and property.
- F. Violence in the workplace is a growing problem in healthcare. It is necessary to develop a program to address workplace violence.

III. OBJECTIVES

The Objectives for the Security Program are developed from information gathered during routine and special security assessment activities. Annual evaluation of the previous year's program activities, performance measures, dashboards, environmental tours and collaboration from other Prisma Health Richland facilities are essential to determine trends that help reduce or prevent crime.

Objectives for this Plan are:

- 1) Service: Conduct a minimum of 12 Active Shooter Presentations and/or Comprehensive Security Assessments
- 2) Quality: Improve Staff and Patient safety in Women's Service as it pertains to security related issues. Special attention given to Infant Security.
- 3) Achieve and maintain an emergency response time of less than four minutes for all emergency responses. Four minutes being the national average for emergency response referenced in the NFPA Standard 1710
- 4) Quality: Conduct a minimum of 6 CPI classes

IV. ORGANIZATION AND RESPONSIBILITY

- A. The Board of Trustees receives regular reports of the activities of the Security Program from our multidisciplinary Environment of Care Committee, which is responsible for the Physical Environment issues. They review reports and, as appropriate, communicate concerns about identified issues and regulatory compliance. They also provide financial and administrative support to facilitate the ongoing activities of the Security Program.
- B. The Operations Executive (OE) and the Chief Executive Officer (CEO) receive regular reports on the activities of the security program. The OE and CEO collaborate with the Director and Manager of Security Services to establish operating and capital budgets for the security program.
- C. The Director and Manager of Security Services work under the general direction of the OE and CEO. The Director and Manager of Security Services, in collaboration with the Environment of Care Committee and other department Directors' are responsible for directing and monitoring all aspects of the security program. The Director and Manager of Security Services inform the Environment of Care Committee regarding security issues that may necessitate changes to policy, education or expenditure of funds.

The management structure and organization of the security department contains both hospital and contract team members. The Security Manager assists the Director of Security Services with the daily security operations. The contract team members consist

of the security officers from American Security Service. An American Security Service on-site leader reports to the Security Manager and is responsible for the hiring, training and scheduling of the contract security officers. Full-time and part-time security officers are contracted to cover the approximate eighty F.T.E. security positions. The responsibilities of the security officers are to make both interior and exterior patrols of the campus on foot and by vehicle. The Officers respond to emergency and non-emergency calls for assistance. Security policies, security post orders and the S.C. State Code of Laws govern the security officer functions. The duties of Security Officers are further discussed in the American Security Services Post Orders.

- D. Department Directors are responsible for orienting new team members to the department and how to perform job specific security procedures. Department Directors in security sensitive areas are responsible for training their team members in any special security procedures or precautions. When necessary, the Director of Security Services and Security Manager will provide department Directors with necessary assistance in developing department security programs or policies.
- E. Individual team members are responsible for learning and implementing job and task specific procedures for security operations.

V. PERFORMANCE ACTIVITIES

The performance measurement process is one part of the evaluation of the effectiveness of the Security program. The performance indicators have been established to measure several aspects of the Security Program. These indicators will be reported monthly on the Security Management section of the Environment of Care Dashboard. The current performance indicators for the Security program are:

- Arrest
- Assaults
- Disturbances
- Infant Abduction System Drills
- Loss of Property
- Thefts of Property
- Vehicle Theft
- Vehicle Breaking & Entering

VI. PROCESSES MANAGING SECURITY RISK

Management Plan

The hospital develops, maintains, and annually evaluates the effectiveness of the Security Management Plan to ensure we are effectively managing the security risks as it relates to team members, visitors, and patients at Prisma Health Richland.

Security Assessments

The Director of Security Services, with the assistance of the Security Manager, implements the security assessment process for Prisma Health Richland and offsite facilities. The Director and Manager of Security Services are designated to manage security risk, coordinate security risk reduction activities in the physical environment, collect deficiency information, and disseminate summaries of actions and results. The Director and Manager of Security Services assure compliance with applicable codes and regulations. The Director of Security Services and the Security Manager develop and maintain the Security Management Plan. On an annual basis, they evaluate the scope, objectives, performance, and effectiveness of the Plan to manage the security risk of the team members, visitors, and patients at Prisma Health Richland.

The hospital identifies security risks associated with the environment of care. Risks are identified from internal sources such as ongoing monitoring of the environment, results of root cause analyses, results of annual proactive risk assessment of high-risk processes, and from credible external sources such as Sentinel Event Alerts.

The security assessment is used to evaluate the impact of the environment of care on the ability of the hospital to perform clinical and business activities. The impact may include disruption of normal functions or injury to individuals. The assessment will evaluate the risk from a variety of functions, including structure of the environment, the performance of everyday tasks, workplace violence, theft, infant abduction, and unrestricted access to medications or other security sensitive areas.

Use of Security Assessment Results

A Security Assessment is used to evaluate the impact of the environment of care on the ability of the hospital to perform clinical and business activities. Where risks are identified, the current programs and processes to manage those risks are compared to the risks that have been identified. Where the identified risks are not appropriately handled, action must be taken to eliminate or minimize the risk. The actions may include creating new programs, processes, procedures and training programs. Monitoring programs may be developed to assure the risks have been controlled to achieve the lowest potential for adverse impact on the security of patients, team members, and visitors.

I. D. Program

The Director and Manager of Security Services are responsible for coordinating the identification program. The Human Resources Director, Security Services Director and Manager, along with security personnel and all supervisory team members are responsible for managing the identification program.

Hospital administration with input from Human Resources and Security Services will develop policies for identification. Both organizational and individual departmental security policies are reviewed at intervals set forth by Administration. Additional interim reviews may be performed as needed. The Director and Manager of Security Services will review organization wide security policies. The Director and Manager of Security Services, with assistance from department Directors, will review departmental security policies.

All team members are required to display their issued identification badge on their upper body with the picture showing while on duty. Director and Manager of Security Services, security personnel and all supervisory team members are responsible for enforcing identification policies. Violations of identification policies involving team members are reported to the individual's direct supervisor. Identification badges are retrieved from personnel upon termination and terminated in the systems.

Patient identification is provided by Patient Access Services at the time of admission. If a patient's wristband is damaged it is replaced by the nursing team members. Patient identification is not removed upon discharge. Patients are instructed to remove the identification band at home. Violations of identification policies involving patients are reported to the nursing unit. Additional protective steps are taken to identify infants on Women and Children Services.

Visitors presenting during normal visiting hours are not required to obtain permission to proceed to the patient's room. Visiting after normal visiting hours requires visitors to provide proper identification and sign in at the security desk. The security officer will call the nursing unit for the floor that the patient is located to obtain authorization for the visitor. If permission is granted, then the visitor may proceed to the patient's room. If not, the visitor is directed to return during normal visiting hours.

Corporate Purchasing provides vendor identification. Facilities Management Department requires contractors to provide identification for all their team members on site.

Sensitive Areas

The Director and Manager of Security Services work with leadership to identify security sensitive areas by utilizing security assessments and analysis of incident reports. The following areas are identified as sensitive: ATM Area, Administration, Gift Shop, Cashier Areas, Central Energy Plant/Engineering, Credit Union, Emergency Department, Laboratory/Morgue, Health Information, Information Technology, Patient Access, Perioperative Services, Pharmacy, Behavioral Health, Security Safe Room, Women Services, NICU, Nurseries and ICU/CCU.

Personnel are reminded during their annual in-service about those areas of the facility that have been designated as sensitive. Personnel assigned to work in sensitive areas receive department level continuing education on an annual basis that focuses on special precautions or responses that pertain to their area.

The Director and Manager of Security Services coordinates the development of hospital-wide written security policies and procedures, and provides assistance to department heads in development of departmental security procedures, as requested. These policies and procedures include infant and pediatric abduction, workplace violence, and other events that are caused by individuals from either inside or outside the hospital.

Individual department heads assist in the development of department-specific security policies and procedures for risks unique to their area of responsibility. The Director and Manager of Security Services also assist department heads in the development of new department security procedures. Hospital-wide security policies and procedures are distributed to all departments. Department heads are responsible for distribution of department level policies and procedures to their team members and for ensuring enforcement of security policies and procedures. Each team member is responsible for following security policies and procedures.

Hospital-wide and departmental security policies and procedures are reviewed at intervals set forth by Administration. Additional interim reviews may be performed on an as needed basis. The Director and Manager of Security Services coordinates the triennial and interim reviews of hospital-wide procedures with department heads and other appropriate team members, and works with department heads to review departmental security policies and procedures.

Security Incident Procedures

The Director and Manager of Security Services coordinate the development of organization-wide written security policies and procedures, and provides assistance to department heads in development of departmental security procedures, as requested. These policies and procedures include infant and pediatric abduction, workplace violence, and other events that are caused by individuals from either inside or outside the organization.

Individual department heads assist in the development of department-specific security policies and procedures for risks unique to their area of responsibility. The Director and Manager of Security Services also assist department heads in the development of new department security procedures. Organization-wide security policies and procedures are distributed to all departments. Department heads are responsible for distribution of department level policies and procedures to their team members and for ensuring enforcement of security policies and procedures. Each team member is responsible for following security policies and procedures.

Organizational and individual departmental security policies and procedures are reviewed at intervals set forth by Administration. Additional interim reviews may be performed on an as needed basis. The Director and Manager of Security Services coordinates the reviews of organization-wide procedures with department heads and other appropriate team

members, and works with department heads to review departmental security policies and procedures.

Security Incident Response

Upon notification of a security incident, the Director and Manager of Security Services or their designee, will assess the situation and implement the appropriate procedures for both emergent and on-emergent security responses. The Director and Manager of Security Services will notify Administration if necessary to obtain additional support. Security incidents that occur in the Emergency Department will be managed initially by the Officer on Duty in the Emergency Department following the appropriate policies and procedures for that area. The Director and Manager of Security Services will be notified about the incident as soon as possible.

Security incidents that occur in the departments will be managed according to the departmental or facility-wide policy. The Director and Manager of Security Services will be notified about any incident that occurs in a department as soon as possible. Additional support will be provided from the Security Department.

In the event of a child reported missing, a Security Alert – Missing Infant/Child is announced over the internal page system, as well as to selected two-way radios and pagers. Designated team member responds to doors and specified areas to observe for persons with children or packages, and call Security if such cases occur. Other team members will check designated areas and respond to the unit involved to document information, and provide support to the parents.

The plan is tested periodically by Emergency Management ensuring appropriate response to the drill. The responses are documented, evaluated, critiqued, and as appropriate corrective activity, additional training, or program improvements are made.

Following any security incident, a written “Security Incident Report” will be filed by the security officer managing the incident. The report will be reviewed by the Security Supervisor and Security Management. Any deficiencies identified in the report will be corrected. A summary of these reports will be furnished to the Environment of Care Committee on a regular basis.

Evaluating the Management Plan

On an annual basis, the Director and Manager of Security Services evaluates the scope, objectives, performance, and effectiveness of the Plan to manage the security risks to the team members, visitors, and patients at Prisma Health Richland. Evaluations are submitted to the Environment of Care Committee for Approval.