

DEPARTMENT: Information Protection and Security	POLICY DESCRIPTION: Physical Security Program
PAGE: 1 of 6	REPLACES POLICY DATED:
EFFECTIVE DATE: February 1, 2019	REFERENCE NUMBER: IP.PS.001
APPROVED BY: Ethics and Compliance Policy Committee	

SCOPE: Company-affiliated hospitals and freestanding emergency departments.
PURPOSE: To establish a framework for the Company's Physical Security Program.
<p>POLICY:</p> <ol style="list-style-type: none"> 1. All employees, physicians, subcontractors, and vendors must carry out their roles and responsibilities in a manner to protect individuals within the facility. 2. Facilities must implement the Company's Physical Security Program. <ul style="list-style-type: none"> • Facilities will implement and monitor compliance with the Company's Physical Security policies and procedures (see Ethics & Compliance site for required model policies). • The Facility will complete a physical security risk assessment minimally every two years to identify internal and external security threats and vulnerabilities, defining critical functions necessary to continue the organization's operations, defining the controls in place necessary to reduce exposure, and evaluating the cost of such controls. The risk assessment should include security staffing model and workforce education. • Facilities will comply with the Company's Physical Security minimum equipment standards and guidelines or have a mitigation plan in place until compliant. • Each Facility Security Program will align with the Company's and Facility's Emergency Preparedness and Operations program. • Facilities will implement LiveSafe as a security incident and near miss reporting tool for their workforce. Workforce members with company-owned mobile phone devices or mobile phone devices that are used for HCA business purposes will have LiveSafe installed.
<p>PROCEDURE:</p> <ol style="list-style-type: none"> 1. Facilities will implement a Physical Security Program that identifies: <ol style="list-style-type: none"> a. Governance/Leadership b. Risk Assessment and Reporting c. Security Staffing and Workforce Education d. Physical Security Equipment e. Emergency Preparedness and Management

DEPARTMENT: Information Protection and Security	POLICY DESCRIPTION: Physical Security Program
PAGE: 2 of 6	REPLACES POLICY DATED:
EFFECTIVE DATE: February 1, 2019	REFERENCE NUMBER: IP.PS.001
APPROVED BY: Ethics and Compliance Policy Committee	

2. Governance/Leadership will, at a minimum, include:

Facility leadership will identify a Security Administrator to manage the Physical Security Program for the facility. The Security Administrator should possess the authority to immediately and independently address any imminent threat that may result in serious injury, death, or significant loss of property. The authority should include standing authorization to deploy and implement timely interim measures. The designated Security Administrator is responsible for providing and engaging security expertise and the following:

- a. Directing implementation and compliance with the Company's Physical Security policies and procedures (hyperlink to required policies);
- b. Hiring necessary security personnel
- c. Developing and providing training on all aspects of security practices and responsibilities;
- d. Issuing security equipment to staff
- e. Obtaining and maintaining physical and electronic security equipment and technology;
- f. Engaging all staff in the security program;
- g. Interacting with patients, visitors, the community and first responders for security related issues;
- h. Managing security-related and violence prevention policies;
- i. Complying with industry standards, regulatory requirements, and appropriate guidelines;
- j. Conducting Security Risk Assessments including providing recommendations to include monitoring and corrective action reporting; and
- k. Identifying, collecting, and evaluating security analytics to make evidence-based decisions.

3. Risk Assessment

- a. The facility risk assessment should include consideration of:
 - 1) Threats to employees, physicians, visitors, family and non-employed support personnel;
 - 2) Patient census, case mix and acuity levels;
 - 3) The type, volume, and severity of criminal activity occurring in and around the facility;
 - 4) The need to provide services to crime victims as well as the impact of patients in police or corrections custody;

DEPARTMENT: Information Protection and Security	POLICY DESCRIPTION: Physical Security Program
PAGE: 3 of 6	REPLACES POLICY DATED:
EFFECTIVE DATE: February 1, 2019	REFERENCE NUMBER: IP.PS.001
APPROVED BY: Ethics and Compliance Policy Committee	

- 5) The physical environment, including the number and size of buildings, equipment, medical gases, and utilities;
- 6) Intangible assets, such as business records, electronic data and any other information assets;
- 7) Cash; and
- 8) Status of training provided to workforce.

4. Reporting

- a. Each facility must develop and adopt a Security Incident and Near Miss Reporting model policy.
- b. Workforce members are required to report a security incident for all adverse security-related occurrences to include, but not be limited to, events occurring on facility property such as assaults/battery, burglary, thefts, robbery, violent acts, and combative persons and other security near misses and events.
 - 1) The facility should investigate and document all security-related occurrences using Incident Reports.
- c. On a routine basis throughout the year, the Security Administrator should review security incident categories, trends, and severity to identify performance improvement activities.
- d. On an annual basis, the Security Administrator should evaluate security incident trends to develop goals and update the facility Security Management Plan.

5. Security Staffing and Workforce Education

- a. Each facility shall develop a staffing model based on the results of its security risk assessment weighing responsiveness and preventative posture. Facility risk assessment includes:
 - 1) Duties and expectations
 - 2) Service response time
 - 3) Patrol frequency
 - 4) Routine and non-routine activities
- b. Patient volume, mix and acuity, if applicable.

DEPARTMENT: Information Protection and Security	POLICY DESCRIPTION: Physical Security Program
PAGE: 4 of 6	REPLACES POLICY DATED:
EFFECTIVE DATE: February 1, 2019	REFERENCE NUMBER: IP.PS.001
APPROVED BY: Ethics and Compliance Policy Committee	

- c. Crime analysis based on the type and volume of criminal activity occurring in and around the facility. The need to provide services to crime victims as well as the impact of patients in police or corrections custody.
 - d. Number of locations or size of facility footprint and security sensitive areas.
 - e. Facility security incident activity, history and environmental conditions to include severity and frequency.
 - f. All workforce members have responsibilities that contribute to a safe and secure environment and should be educated on the following:
 - 1) How to contact Security or Security Administrator;
 - 2) What and how to report security issues or incidents to Security or Security Administrator;
 - 3) LiveSafe; The importance of displaying and checking identification;
 - 4) Procedures for preventing and responding to emergency situations including, but not limited to, abductions, breaches and workplace violence;
 - 5) Preventing, intervening, reporting and resolving workplace violence issues; and
 - 6) Their role in crime prevention.
 - g. Personal safety awareness. All workforce members must receive security education within thirty (30) days of employment.
 - h. All workforce members must receive annual physical security education.
 - i. Workforce members in security sensitive areas (e.g., pediatrics, behavioral health, ICU) must receive education specific to the security risks in those areas. If assigned to a security sensitive area, such specialized training should occur prior to the first unsupervised assignment.
 - j. Expectations related to the role of workforce in the physical security program should be reinforced and available within facility policies, procedures and employee handbooks.
6. Physical Security Equipment
- a. Physical security equipment and enhancements should be deployed after conducting a security risk assessment.
 - b. The use of security equipment safeguards should have a defined purpose, policy and procedure and align with Company standards.

DEPARTMENT: Information Protection and Security	POLICY DESCRIPTION: Physical Security Program
PAGE: 5 of 6	REPLACES POLICY DATED:
EFFECTIVE DATE: February 1, 2019	REFERENCE NUMBER: IP.PS.001
APPROVED BY: Ethics and Compliance Policy Committee	

- c. The number and type of physical security safeguards used in the facility may vary. Using crime prevention through environmental design (CPTED) principles for layered protection, the following systems may be implemented:
 - 1) Access control to include doors, locking mechanisms, key systems and electronic access technologies;
 - 2) Video surveillance to include cameras, monitoring devices, recording equipment and video intercoms;
 - 3) Communication devices to include radio communications, dispatching equipment and software, emergency call boxes and mass notification devices;
 - 4) Screening equipment to include visitor management and metal detection;
 - 5) Asset protection to include equipment used to safeguard narcotics, cash, weapon storage, safes and lockboxes;
 - 6) Patient and asset tracking to include infant protection, elder and high risk patient monitoring and Radio Frequency ID (RFID) tags;
 - 7) Use of CPTED principles to include fencing, lighting, landscaping, window glazing and workspace design; and
 - 8) Psychological deterrents to include security signage, wayfinding guidance and clearly marked security vehicles.
- d. The facility must provide workforce members guidance and education regarding each of these systems.
- e. The facility must ensure the systems are in working order and regularly test the systems and repair or replace as necessary.
7. Emergency Management
 - a. The Security Administrator should participate in the facility's multidisciplinary emergency management team to represent and support the security function.
 - b. The Security Administrator should participate and provide input to the facility's comprehensive hazard/risk vulnerability analysis (HVA).
 - c. Multidisciplinary emergency response policies, procedures and plans should include and address security mitigation, preparedness, response and recovery.
 - d. Emergency policies, procedures and plans should address immediate, short-term and long-term response for security.

DEPARTMENT: Information Protection and Security	POLICY DESCRIPTION: Physical Security Program
PAGE: 6 of 6	REPLACES POLICY DATED:
EFFECTIVE DATE: February 1, 2019	REFERENCE NUMBER: IP.PS.001
APPROVED BY: Ethics and Compliance Policy Committee	

- e. The Security Administrator should participate in facility after action debriefs to provide input and feedback.

REFERENCES:

1. The Joint Commission
2. International Association for Healthcare Security & Safety
3. Facility Model Physical Security Program Policies at:
<http://connect.medicity.net/web/physicalsecurity/policies>