City and County of San Francisco
Edwin M. Lee
Mayor

San Francisco Health Commission

DEPARTMENT OF PUBLIC HEALTH, - SECURITY REPORT

Basil A. Price, Director of Security
basil.price@sfdph.org

SAN FRANCISCO HEALTH COMMISSION
DEPARTMENT OF PUBLIC HEALTH, 2015-2016 SECURITY REPORT
January 5, 2016, Basil Price, DPH Director of Security

SFDPH CLINICS	
SECURITY ASSESSMENT KEY FINDINGS	**KEY RECOMMENDATIONS**
I. CLINIC ELECTRONIC SECURITY SYSTEM	
Systems and Devices • The use of electronic security systems is inconsistent throughout DPH Clinics. There is no standardization. There are differing types of security system design applications that have been installed over the years including push button locks, help buttons, and dummy cameras, creating non-uniform security system practices. • Those DPH Clinics that currently have security system and devices installed have multiple access control systems, which are controlled by the various Facilities Department, under the discretion of the Facility Director. Where systems are in place, they appear to be functional, and most card readers are in working order. However, there are no system inspection and maintenance reports to ensure functionality. The systems reporting function does not easily identify which components are working properly, which allows for the potential of device failures without proper follow-through. System Operational Issues • Video surveillance is not installed in many security sensitive areas, as required by healthcare security industry standards, for the purpose of recording and digital archiving. • There are inactive intruder alarm systems with motion detection installed that are no longer being monitored. The clinics do not comply with healthcare security system standards. Access Control • Exterior doors throughout the clinics are not consistently monitored by exterior cameras. Many stairwell doors can be opened from the exterior of the buildings, and several allow unrestricted access into patientcare areas. • Not all clinics are equipped with card readers. In some instances, rear entry doors were propped open for ventilation purposes, creating a security vulnerability to the workplace.	Electronic Security System Recommendations • Update all building security systems and devices to current healthcare security industry standards. • Develop a security-by-design process where the Director of Security is involved in the security systems designs associated with remodel of existing buildings and construction of new facilities. • The existing access control, alarm, and CCTV systems should be replaced with a new Lenel security management system on a phased approach in accordance with budget availability and identified useful lifespan of the existing systems. • Security systems should be integrated between all DPH Hospitals, Clinics, Behavioral Health Facilities, and Administration Buildings to improve system management, enhance customer service, and provide operational efficiencies. • All systems should utilize DPH local and wide-area networks as communications paths, thus reducing infrastructure costs while improving operational features and efficiencies. Provisions should be made to support future system expansions, including connection to all of the off-site buildings for local and remote monitoring and reporting. • Develop a comprehensive program to manage the security electronic systems, including monthly testing of all systems, budget planning, administration, service, maintenance, and repair of security equipment, including periodic software upgrades. • Develop a phased approach to add doors, gates, and/or enclosed counters to inner lobby access areas and reception desks that are currently open to provide securable entry points for employees only. • Increase annual maintenance and service budget to a level that is sufficient to repair and maintain all dysfunctional devices and systems. • All buildings should incorporate access control, alarm monitoring, and closed circuit television.

SFDPH CLINICS

SECURITY ASSESSMENT KEY FINDINGS	KEY RECOMMENDATIONS
• The physical design of many of the clinics does not funnel visitors to staffed reception areas where assistance, general guidance, and a psychological deterrence to wrong direction, or wrong doing can be provided. • There are no physical barriers to clearly distinguish between public areas and work areas. • The employee entry areas are not equipped with access control functionality. <u>Alarm Systems</u> • Several buildings have no electronic security systems whatsoever. Others have installed monitoring equipment that is inoperable. Alarm monitoring is inconsistent in its application with different system manufactures, including buildings where there is no access control system installed. • Most of the cash handling areas are not equipped with appropriate safes, and cash drawers, and cash transactions are not monitored by video surveillance, and have no alarm system. <u>ID Badge System</u> • Production of ID badges is the function of the Human Resources Department, and the programming of badges is the function of the Facilities Department. There is no collaboration or communication between the departments, resulting in terminated employees with active badges in the proximity card system. • The wearing of photo ID badges by employees is inconsistent. <u>CCTV Systems</u> • The CCTV system technology is outdated and needs replacing. The camera coverage is also inadequate. The CCTV System cannot fully contribute to customer service objectives due to inherent limitations of information provided.	• All future cameras, card readers, and alarms should be connected to the new systems. • Remove and/or replace all existing equipment that is non-functional. • All alarms are to be tested at least monthly, and reported to the DPH Director of Security quarterly, include action plans to addressing malfunctioned equipment. • All cameras should be "called up" and tested for proper view of intended area as well as quality of picture. Inadequate images should be identified and trouble-shooting should be conducted. Any dysfunctional cameras should be replaced immediately. • All emergency phones should be equipped with camera call up availability at the responding SOC. • All perimeter doors should be alarmed and monitored by the security system. • All emergency exit doors and/or stairwell doors that can be opened from the exterior of the building should be locked from the outside and equipped with local internally mounted sounders. • All exterior stairwell exit doors should be equipped with cameras which monitor the doors with automatic camera call-up if the local sounder is activated. • All interior doors to employee areas should be closed and secured. • Push button locks should be standardized and codes changed regularly. • All Help Buttons should be consistent in design and application. Testing of working help buttons should be completed at least monthly. All help buttons should be integrated between all DPH Hospitals, Clinics, Behavioral Health Facilities, and Administration Buildings, and ring into the dispatch center at SFGH to provide adequate response, improve system management, enhance customer service, and provide operational efficiencies.

SFDPH CLINICS	
SECURITY ASSESSMENT KEY FINDINGS	**KEY RECOMMENDATIONS**
Support and Maintenance • DPH Facilities staff and contract technicians are equipped with the proper system knowledge for trouble-shooting; however, there is no administrative oversight to manage systems DPH-wide.	System Installation • DPH commitment to a plan for equipment and technology enhancements – cameras, security hardware and networking for all DPH facilities. • In collaboration with the DPH Director of Security, Facilities, and DPH IT, develop a project to bring all DPH facilities to healthcare security industry standards. Operations Recommendations • Improve the current communications system, including help-buttons so that is capable of radio and telephone communications between all DPH facilities. • Develop a comprehensive security training program that includes Nonviolent Crisis Intervention. • Develop a security awareness program. The program should have measurable goals that are reported to the DPH Director of Security on a quarterly basis. • Encourage all employees to wear ID badges during working hours and to keep doors closed and locked. • Develop a Threat Management Team to develop safeguards that cover all persons, patients, visitors, employees, and physicians, by addressing threats and aggressive behavior at the earliest stage; defining inappropriate and unacceptable workplace behavior; and establishing an effective process for responding to, managing, and reporting acts or threats of violence or aggressive behavior. • All ID Badge Services, including production, programming, and producing badge audit-history reports to be performed by DPH Security Services Department. • Implement a security incident reporting process, where DPH security incidents are documented in a DPH Incident management program that has activity tracking capability for trending and analysis.

SFDPH CLINICS	
SECURITY ASSESSMENT KEY FINDINGS	**KEY RECOMMENDATIONS**
II. CLINIC SECURITY STAFFING	
Security Staffing • The San Francisco Sheriff's Department (SFSD) is the contract security provider for DPH; however, physical security is inconsistent at the clinics. Some security services are provided by SFSD, some by private security companies, and others have no uniformed security presence.	Staffing Recommendations • Hire a full-time proprietary Security Systems Administrator with overall responsibility for the oversight of the implementation of hospital's security systems and technology integration. • Hire a full-time proprietary Security Manager with responsibility for clinic security oversight. • Ensure that baseline SFSD security staffing levels assigned to DPH can accommodate account management, supervision, basic security patrolling requirements of the clinic's interior, exterior, and provide for mutual back up. • Additional security staffing considerations to address the following: 1. Demographic composition, geographic location, and the severity of criminal acts confronting a facility. 2. Security Sensitive Areas
III. CLINIC EMPLOYEE SECURITY AWARENESS	
Security Operations and Security Awareness • Where SFSD provides security services, incident reports are entered into a SFSD databased, which DPH has no access. Copies of incident reports require a written request to the Office of the Sheriff. In the incident is under criminal investigation, DPH may not be provided a copy. • Security incident data for trending, risk mitigation is inconsistent, and cannot be validated for accuracy. There is not a central Unusual Occurrence Reports (UO) system, with guidelines for documenting security related incidents. There is no UO system analysis to properly categorize incidents, and conduct security incident trending by facility.	Clinic Employee Security Awareness Recommendations • Develop security operations procedures specific to each DPH Clinic. • Develop security response procedures to address security emergencies.

SFDPH CLINICS	
SECURITY ASSESSMENT KEY FINDINGS	**KEY RECOMMENDATIONS**
• Employee Security Awareness at the clinics is marginal. The majority of clinics do not have written security response plans, including quarterly security drills to monitor security program effectiveness, and staff proficiency.	

LAGUNA HONDA HOSPITAL AND REHABILITATION CENTER	
SECURITY ASSESSMENT KEY FINDINGS	**KEY RECOMMENDATIONS**
I. LHH LEADERSHIP SUPPORT	
Leadership Support The LHH leadership has supported the security program through implementation of the following: • Protocol for timely notification of sentinel events to LHH and SFDPH leadership. • Monthly meetings with LHH Administrator and the Director of Security, to identify security vulnerabilities, and begin developing the infrastructure for an effective and comprehensive security program at LHH. • Included the Director of Security, in LHH Executive Committee, Safety, and Leadership Meetings. From a security perspective, Laguna Honda Hospital and Rehabilitation Center has a set culture of being reactive instead of proactive to security risk and vulnerabilities. Interviews with staff reveal that the hospital's security vulnerabilities have been common knowledge with employees for several years. Many employees expressed that do not feel safe because reports of security and safety hazards have gone without a response. Many of LHH antiquated security related systems and process create barriers in bring LHH to healthcare community standards, and effecting positive change.	LHH Leadership Support Recommendations • Establish regular security leadership meetings to address all security related issues, including accountability to the contract security provider. • Develop a Threat Management Team to develop safeguards that cover all persons, patients, visitors, employees, and physicians, by addressing threats and aggressive behavior at the earliest stage; defining inappropriate and unacceptable workplace behavior; and establishing an effective process for responding to, managing, and reporting acts or threats of violence or aggressive behavior. • Implement a security incident reporting process, where LHH incidents are documented in a LHH incident management program that has activity tracking capability for trending and analysis. • Revise the UO System to allow for security incident reporting of all crimes against persons and facility property, in-order to track activity for trending and analysis.

LAGUNA HONDA HOSPITAL AND REHABILITATION CENTER

SECURITY ASSESSMENT KEY FINDINGS	KEY RECOMMENDATIONS
II. LHH ELECTRONIC SECURITY SYSTEM	
Systems and Devices LHH currently uses multiple access control systems, which are controlled by the Facilities Department. The system appears to be functional and most card readers are in working order. However, there are no system inspection and maintenance reports to ensure functionality. The systems reporting function does not easily identify which components are working properly, which allows for the potential of device failures without proper follow-through. Video surveillance, help buttons, alarms, and emergency security phones were not all in working order, and do not ring into the Security Operations Center for appropriate assessment and response. System Operational Issues • There are differing types of security system design applications that have been installed over the years including push button locks, help buttons, video surveillance cameras, creating non-uniform security system practices. • Video surveillance is not installed in many security sensitive areas, as required by healthcare security industry standards, for the purpose of recording and digital archiving. • There are inactive intruder alarm systems with motion detection installed that are not being monitored by the Security Operations Center. • Emergency Security Phones are installed around the buildings perimeter, which are not operational.	Electronic Security System Recommendations • Update all building security systems and devices to current healthcare security industry standards. • Develop a security-by-design process where the Director of Security is involved in the security systems designs associated with remodel of existing buildings and construction of new facilities. • The existing access control, alarm, and CCTV systems should be replaced with a new Lenel security management system on a phased approach in accordance with budget availability and identified useful lifespan of the existing systems. • Security systems should be integrated between all DPH Hospitals, Clinics, Behavioral Health Facilities, and Administration Buildings to improve system management, enhance customer service, and provide operational efficiencies. • All systems should utilize DPH local and wide-area networks as communications paths, thus reducing infrastructure costs while improving operational features and efficiencies. Provisions should be made to support future system expansions, including connection to all of the older buildings for local and remote monitoring and reporting. • Develop a comprehensive program to manage the security electronic systems, including monthly testing of all systems, budget planning, administration, service, maintenance, and repair of security equipment, including periodic software upgrades. • Develop a phased approach to add doors, and enclosed the Human Resource Department, including counters to inner lobby access areas and reception desks that are currently open, to provide securable entry points for HR employees only. • Increase annual maintenance and service budget to a level that is sufficient to repair and maintain all dysfunctional devices and systems. • All buildings should incorporate access control, alarm monitoring, and video surveillance.

LAGUNA HONDA HOSPITAL AND REHABILITATION CENTER

SECURITY ASSESSMENT KEY FINDINGS	KEY RECOMMENDATIONS
Access Control • Exterior doors throughout the old building are easily defeated, some were found unsecured, and are not currently monitored by video surveillance. • The lack of a visitor access control process, including screening, and photo identification passes, create opportunity for unauthorized building access, including resident neighborhoods. • The loading dock does not restrict access. Access to the ancillary departments doors are easily compromised, and need replacing. • The rear entry doors to the older buildings are often propped open, allowing access into the facility, including ancillary work areas. • Several exterior doors, windows, and air-vents are compromised to gain access. Alarm Systems • Several buildings (older buildings) have no electronic security systems whatsoever. Others have installed monitoring equipment that is inoperable. Alarm monitoring is inconsistent in its application with different system manufactures, including the pharmacies, and buildings where there is no access control system installed. • Most of the cash handling areas are not equipped with safes, and cash drawers, and cash transactions are not monitored by an alarm system or video surveillance. ID Badge System • Production of ID badges is the function of the Human Resources Department, and the programming and producing of badges is the function of the Facilities Department. There is no collaboration or communication between the departments, resulting in terminated employees with active badges in the proximity card system.	• All future and existing electronic security systems, should ring into the San Francisco General Hospital's Security Operations Center. • Remove and/or replace all existing equipment and emergency phones that are non-functional. • All alarms are to be tested at least monthly, and reported to the Safety Committee quarterly, including action plans to addressing malfunctioned equipment. • All cameras should be "called up" and tested for proper view of intended area as well as quality of picture. Inadequate images should be identified and trouble-shooting should be conducted. Any dysfunctional cameras should be replaced immediately. • All emergency phones should be equipped with camera call-up availability at the responding SOC. • All perimeter doors should be alarmed and monitored by the security system. • All emergency exit doors and/or stairwell doors that can be opened from the exterior of the building should be locked from the outside and equipped with local internally mounted sounders. • All exterior stairwell exit doors should be equipped with cameras which monitor the doors with automatic camera call-up if the local sounder is activated. • All interior doors to employee areas should be closed and secured. • Push button locks should be standardized and codes changed regularly. • All help buttons should be consistent in design and application. Testing of working help buttons should be completed at least monthly.

LAGUNA HONDA HOSPITAL AND REHABILITATION CENTER	
SECURITY ASSESSMENT KEY FINDINGS	**KEY RECOMMENDATIONS**
CCTV Systems • The CCTV system technology is outdated and needs replacing. The camera coverage is also inadequate. The CCTV System cannot fully contribute to customer service objectives due to inherent limitations of information provided. Support and Maintenance • Contract technicians are equipped with the proper system knowledge for trouble-shooting; however, proprietary oversight to manage the system vendor is limited.	Operations Recommendations • Improve lighting at Building 1 South Road, and increase evening and night security patrols. • Improve the current communications system, including help-buttons so that it is capable of communication and response between all SFGH and LHH facilities. • Upgrade the audio recorder that records all SOC operator phone communication. • Immediately schedule proper training of SOC staff, and DPH personnel on retrieving video surveillance footage. • Develop a comprehensive security training program that includes, Crisis Intervention, Trauma Informed Care, Care Experience Training, and Crisis Response Training. • Develop an employee security awareness program. The program should have measurable goals that are reported to the Safety Committee, quarterly. Encourage all employees to wear ID badges during working hours and to keep doors closed and locked. • Develop a Threat Management Team to develop safeguards that cover all persons, residents, visitors, employees, and physicians, by addressing threats and aggressive behavior at the earliest stage; defining inappropriate and unacceptable workplace behavior; and establishing an effective process for responding to, managing, and reporting acts or threats of violence or aggressive behavior. • Security Services, should have the ability to deactivate, and grant access, and lockdown the facility via the SOC, including producing badge audit-history reports. • Implement a security incident reporting process, where LHH incidents are documented in a SFGH incident management program that has activity tracking capability for trending and analysis. • Develop a monthly survey to monitor the contract security provider's compliance with specified MOU performance measures.

LAGUNA HONDA HOSPITAL AND REHABILITATION CENTER	
SECURITY ASSESSMENT KEY FINDINGS	**KEY RECOMMENDATIONS**
	• Hold weekly meetings with hospital leadership and the contract security provider's account management to address identified challenges/concerns in real time.
III. LHH SECURITY STAFFING	
<u>Security Staffing</u> The San Francisco Sheriff's Department (SFSD) is the contract security provider. Formal Security Operations Center (SOC) staff systems training for access control, alarm response, and CCTV systems do not currently exist. As a result, only limited employees have SOC system's knowledge, while others adopted a "learn as you go" procedure in using the systems. • All security incident reports are entered into a SFSD databased, which LHH has no access. Copies of incident reports require a written request to the Office of the Sheriff. If the incident is under criminal investigation, LHH may not be provided a copy. • Security incident data for trending, risk mitigation, and performance metrics, is not reported to LHH. The UO system does not allow for specific reporting of all security related incidents, and data is not categorized to determine incident frequency. • The SFSD are responsive to security emergencies; however, hospital staff have expressed concern regarding security visibility, cooperation during LHH security related investigations.	<u>Staffing Recommendations</u> • Hire a full-time proprietary Security Systems Administrator with overall responsibility for the oversight of the implementation of hospital's security systems and technology integration, including responsibility for the following: • Ensure that baseline SFSD security staffing levels assigned to LHH can accommodate account management, administrative level supervision, basic security patrolling requirements of the facility's interior, campus exterior, and provide for mutual back up. • Additional security staffing considerations to address the following: 1. Demographic composition, geographic location, and the severity of criminal acts confronting a facility. 2. Security Sensitive Areas

LAGUNA HONDA HOSPITAL AND REHABILITATION CENTER	
SECURITY ASSESSMENT KEY FINDINGS	**KEY RECOMMENDATIONS**
IV. LHH EMPLOYEE SECURITY AWARENESS	
Security Operations and Security Awareness • The security awareness of the hospital staff is marginal. Historically, LHH has solely depended upon SFSD to develop, implement, and manage the security operation. • The existing security awareness program for employees consists of monthly SFSD security alerts, and periodic SFSD community policing events. • The security information in New Employee Orientation Program is limited, and should be presented by a representative of the Security Department to ensure that all employees will receive basic information related to the Security Department and its Security Management Plan. • During the security portion of the orientation, employees should receive information about the following: 1. A description of the Security department 2. Security services provided 3. Prudent security practices 4. Violence in the Workplace Policy 5. ID Policy 6. Emergency procedures to be followed during security incidents 7. Processes to minimize security risks in sensitive areas 8. Reporting a security incidents or suspicious activity 9. Security command structure 10. Facility response to security related emergencies. 11. Security locations and phone numbers	LHH Employee Security Awareness Recommendations • Develop security operations procedures specific to each DPH Clinic. • Develop security response procedures to address security emergencies.

SFGH SECURITY MANAGEMENT PLAN Q1, FY 2015-2016	
SECURITY STANDARD AND PERFORMANCE METRIC	**ACTUAL PERFORMANCE AND ANALYSIS OF PERFORMANCE METRIC RESULTS**
I. SFGH - CODE GREEN, "AT RISK" PATIENT ALERT RESPONSE DRILLS	
Standard: On at least a quarterly basis, the hospital will conduct a Code Green drill, to determine the effectiveness in the following areas: • Initial Perimeter and Search • AOD Response and Code Green Activation • Hospital-wide Activation and Search • Clearing Code Green **Performance Metric:** The hospital will be measured on its ability to prevent/return an "At Risk" patient: **Prevent/Return-rate Threshold –90%** **Prevent/Return-rate Target – 98%** **Prevent/Return-rate Stretch – 100%** The hospital will be measured on its ability to respond to a hospital-wide activation and search. Hospital personnel should respond according to the Code Green Policy. **Response-rate Threshold – 80%** **Response-rate Target – 90%** **Response-rate Stretch – 100%**	**Actual Performance:** • The hospital will be measured on its ability to prevent/return an "At Risk" patient – 100% • The hospital will be measured on its ability to respond to a hospital-wide activation and search. Hospital personnel should respond according to the Code Green Policy – 14% **Analysis of Performance Metric Results:** The data for the Q1 FY 2015-2016 is based on actual Code Green Incidents. There were no facility-wide drills conducted during Q1, due to the reorganizing of the Code Green Committee. There were a total of seven actual Code Green incidents, which hospital staff responded to one of the events, and successfully returning the patient to the unit. The Sheriff's Department responded, and successfully returned 100% of all AWOL and At Risk patients to the unit. The AeroScout patient tracking system continues to be the contributing factor in locating AWOL and "At Risk" patients.

SFGH SECURITY MANAGEMENT PLAN Q1, FY 2015-2016	
SECURITY STANDARD AND PERFORMANCE METRIC	**ACTUAL PERFORMANCE AND ANALYSIS OF PERFORMANCE METRIC RESULTS**
II. SFGH – CUSTOMER SATISFACTION	
Standard: In accordance with the scope of the security management plan, the management plan calls for best in class customer service for patients, visitors, and staff. On a monthly basis, a sample size of 100 customers, consisting of patients, visitors, employees, and physicians that had a recent contact with Security, will be surveyed on their experience. Customers will respond, Very Satisfied, Satisfied, Somewhat Satisfied, Dissatisfied, and Very Dissatisfied in the following areas: • Responsive • Treated with dignity and respect • Courteous • Effective • Overall Experience **Performance Metric:** The Security Department will be measured on its ability to achieve a rating of Satisfied- Very Satisfied: **Threshold** - 80% **Target** - 90% **Stretch** – 98%	**Actual Performance:** • The Security Department will be measured on its ability to achieve a rating of Satisfied- Very Satisfied. – 66% **Analysis of Performance Metric Results:** During Q1 FY 2015-2016, 100 customers were surveyed regarding their experience with the security department, overall, 66% of the customers rated the department's service as being satisfactory or above. The security department was scored highest in courtesy, and lowest in responsiveness. Based on the verbatim customer comments, efforts to improve the customer's perception by integrating law enforcement services with the care-experience philosophy is paramount. Customer input included the following areas for improvement: • Establish a customer service oriented approach; provide a more caring and friendly experience with skills in de-escalating situations including mental health training with patients, respect and care experience with the family of our patients, and staff. • Increase security visibility by conducting more frequent rounds throughout the campus, at all building interior and exterior, including parking areas. • Improve response time to security emergencies.

SFGH SECURITY MANAGEMENT PLAN Q1, FY 2015-2016	
SECURITY STANDARD AND PERFORMANCE METRIC	**ACTUAL PERFORMANCE AND ANALYSIS OF PERFORMANCE METRIC RESULTS**
III. SFGH – ELECTRONIC SECURITY SYSTEM FUNCTIONALITY	
Standard: On a monthly basis the SOC will inspect every element of the electronic security system for functionality. The Facilities Department will monitor all service call/work-orders to ensure timely response. The Security Director, SFSD Unit Commander will develop a plan to mitigate risk, resulting from system malfunctions. The action plan will be documented in EOC Security Report. **Performance Metric:** **Target**: 100% electronic security system will be inspected, and will be 98% functional.	**Actual Performance:** • One hundred percent of the electronic security system was inspected, and the system is 85% functional. **Analysis of Performance Metric Results:** The security system vendor was contacted to repair all malfunctioning equipment. According to the Facilities Director, service response for the current system's vendor is poor. A meeting was held with the system vendor's branch manager to address the company's performance. A breakdown of the security system's functionality is as follows: **<u>System Evaluation Report</u>** Video Recorders – 97% Alarm Panels – 94% Cameras – 75% Card Readers – 100% Alarm Input/Output – 99% Emergency Phones – 99% Other Input/Output – 99%

SFGH SECURITY MANAGEMENT PLAN Q1, FY 2015-2016	
SECURITY STANDARD AND PERFORMANCE METRIC	**ACTUAL PERFORMANCE AND ANALYSIS OF PERFORMANCE METRIC RESULTS**
IV. DPH and SFSD, MOU PERFORMANCE METRIC	
Standard: A monthly security provider performance survey (SPS). The purpose for the assessment is intended to validate the security provider's compliance with MOU obligations, operational performance, management responsibilities and finance provisions. A value is a weight per item and assigned per line item. The values are to be assigned within a range of "5 to 1" or 0. **Performance Metric:** The provider is expected to maintain scores in the 3-5 range. A score of 1 to 2 indicates that a problem or issue exists that needs to be immediately addressed, and a score of 0 indicates a substantive problem or issue that requires immediate correction or resolution. Each category receives points as achieved per line item. A final numerical score is calculated at the end of the form.	**Actual Performance:** • The provider is expected to maintain scores in the 3-5 range. SFSD average score for Q1 is 4.4. **Analysis of Performance Metric Results:** SFSD has met the target of maintaining an overall score in the 3-5 range for compliance with each category in the MOU. The overall scores for the Q1 FY 2015-2016 were as follows: July – 4.8 August – 4.4 September – 4.2

SFGH SECURITY MANAGEMENT PLAN Q1, FY 2015-2016	
SECURITY STANDARD AND PERFORMANCE METRIC	**ACTUAL PERFORMANCE AND ANALYSIS OF PERFORMANCE METRIC RESULTS**
V. SFGH – CODE PINK INFANT ABDUCTION DRILLS	
Standard: Upon receiving a report of an abduction or attempted abduction or when there is an activation of a portal alarm: The Code Pink Response Procedure will be activated. **Performance Metric:** The hospital will be measured on its ability to prevent an abductor from leaving the facility: **Capture-rate Threshold –90%** **Capture-rate Target – 98%** **Capture-rate Stretch – 100%** The facility will be measured on its ability to respond to a Code Pink. Hospital personnel should be posted at the designated areas, as described in the Code Pink Policy. **Response-rate Threshold – 80%** **Response-rate Target – 90%** **Response-rate Stretch – 100%**	**Actual Performance:** • The hospital will be measured on its ability to prevent an abductor from leaving the facility - 100% • The facility will be measured on its ability to respond to a Code Pink. Hospital personnel should be posted at the designated areas, as described in the Code Pink Policy – 83% **Analysis of Performance Metric Results:** On 9/11/2015, a Code Pink drill was conducted on Ward 6H. The purpose of the drill was to test the overall hospital response, including communications during a Code Pink incident. Observations: ▪ Ward 6H Charge Nurse was able to activate a Code Pink alert using their Unit Specific Code Pink plans. ▪ Rapid securing of hospital perimeter by Sheriff's Department. ▪ Rapid implementation of departmental security and search procedures. ▪ Inaccurate significant event call list phone numbers, and minimal return response by the staff that were notified. ▪ SFSD Radio Operators need additional training on accurate overhead announcements. ▪ Operator overhead announcements need to be reviewed by committee for possible changes in verbiage and frequency. ▪ Overhead speakers require repair. ▪ Numerous units (nine total) called Sheriff's Operation Center to report search results instead of the Code Pink Command Post.

SFGH SECURITY MANAGEMENT PLAN Q1, FY 2015-2016	
SECURITY STANDARD AND PERFORMANCE METRIC	**ACTUAL PERFORMANCE AND ANALYSIS OF PERFORMANCE METRIC RESULTS**
VI. SFGH – USE OF FORCE STATISTICS	
Standard: Monthly data to track SFSD incidents at SFGH that involve the use of force. A breakdown of the data will be as follows: 1. Type of Force 2. Number of incidents. 3. Demographics **Performance Metric:** Significant Reporting Only	**Actual Performance:** • SFGH experienced 51 incidents in Q1, FY 2015-2016, that involved use of force by the SFSD. **Analysis of Performance Metric Results:** **Type of Force:** Discharge Taser - 4 Deploy Taser - 5 Pepper Spray - 2 Deployed Baton - 2 Use of Baton - 2 **Cases:** Patients – 27 Non Patients – 24 Felony Incidents – 12 Misdemeanor Incidents – 16 Mental Health Related Incidents – 18 **Demographics:** Males – 42 Females – 9 Asian/Pacific Islander – 1 Black/African American – 19 Hispanic – 11 White - 19

SFGH SECURITY MANAGEMENT PLAN Q1, FY 2015-2016

SECURITY STANDARD AND PERFORMANCE METRIC	ACTUAL PERFORMANCE AND ANALYSIS OF PERFORMANCE METRIC RESULTS
VII. SFGH – SERIOUS INCIDENT REPORTING	

Standard:

Quarterly data to track SFSD serious incidents at SFGH. Serious incidents are classified as follows:

- Facility Property Thefts (above $950)
- Burglary
- Battery
- Sexual Offense
- Assault
- Robbery
- Homicide

Performance Metric:

Significant Reporting Only

Actual Performance:

Serious Incident Reporting Yearly Comparison	Q1 2014-2015	Q1 2015-2016
SFSD - Facility Theft Reports	16	28
SFSD - Burglary Reports	2	2
SFSD - Battery Reports	15	16
SFSD – Sexual Offense Reports	0	1
SFSD – Assault Reports	4	3
SFSD – Robbery Reports	0	0
SFSD - Homicide Reports	0	0

Analysis of Performance Metric Results:

Comparing the Q1 results from the previous year to the current year, serious incidents increased by 74% (13 incidents). Facility property thefts significantly increased, which contributed to the lack of electronic security systems monitoring the medical office buildings, and thefts of inventory from the ancillary departments.

SFGH SECURITY MANAGEMENT PLAN Q1, FY 2015-2016	
SECURITY STANDARD AND PERFORMANCE METRIC	**ACTUAL PERFORMANCE AND ANALYSIS OF PERFORMANCE METRIC RESULTS**
VIII. SFGH – CAMPUS TUNNEL ACCESS CONTROL	
Standard: Based on the 2015 Security Risk Assessment, the campus tunnels are the hospital's greatest security vulnerability. Security will provide month-to-month and quarterly data to demonstrate the effectiveness of a crime prevention program to minimize or eliminate unauthorized access to the campus tunnels. **Performance Metric:** The report will include the following, as associated with the campus tunnels: • **Arrests** – Number of arrests conducted each month associated with the campus tunnels. • **Crime Analysis** – A monthly break down of criminal incidents reported, associated with the campus tunnels. • **Trespass Warnings** – The number of trespass warnings issued each month associated with the campus tunnels Data gathered in the 2015-2016 report will determine the baseline for the 2016-2017 report.	**Actual Performance:** During Q1 FY 2015-2016, SFSD increased patrols to the hospital tunnels, and made contact with trespassing suspects on two occasions. **Analysis of Performance Metric Results:** Arrest - 1 Crime Analysis – Lodging Trespassing Warnings - 1

SFGH SECURITY MANAGEMENT PLAN Q1, FY 2015-2016	
SECURITY STANDARD AND PERFORMANCE METRIC	**ACTUAL PERFORMANCE AND ANALYSIS OF PERFORMANCE METRIC RESULTS**
IX. SFGH – EMPLOYEE SECURITY AWARENESS	
Standard: Based on the 2015 security risk assessment, employee security awareness is marginal. During EOC rounds, hospital staff be tested on 10 question regarding security. A sample size of 300 employee will be tested each quarter. **Performance Metric:** Target –90% of employees are knowledgeable on regarding security response procedures. Data gathered from the employee surveys will be broken down into the following categories: • Knowledgeable • Partial Knowledgeable • No Knowledge	**Actual Performance:** Knowledgeable— 75% Partial Knowledgeable— 25% No Knowledge— 0