SECTION - SECURITY
ADMINISTRATIVE DIRECTIVE NO. 806
(Replaces A.D. No. 806 dated 1/11/07)

Effective Date: July 2, 2007

SUBJECT: FACILITY SECURITY-STAFF RESPONSIBILITY

I. PURPOSE

This policy establishes staff roles and responsibility for maintaining facility security.

II. AUTHORITY

By authority of the Department of Mental Health (DMH) Special Orders 001.02 and 723, Welfare & Institutions Code Section 4100, and the Health & Safety Code Section 1250.

III. POLICY

A. The maximum-security treatment environment of Coalinga State Hospital (CSH) is designed to be responsive to the needs of the public, Individuals, families, visitors, staff, the courts, and the California Department of Corrections and Rehabilitation (CDCR).

B. Close attention to employees and Individual monitoring is essential for security operations within the facility. Monitoring is the responsibility of all staff behind security, including administrative staff, clinical personnel, Department of Police Services (DPS), and the maintenance staff.

IV. METHOD

A. General Concept:

1. Forensic mental health service, by definition, involves care and treatment of persons with mental disorders that are associated with criminal activity and antisocial behavior. Therefore, in a locked forensic treatment facility, mental health treatment principles must be integrated with effective strategies from police science to create and maintain a safe and secure treatment environment.

2. CSH, as a maximum-security forensic state hospital, necessarily differs in philosophy and orientation from security in a prison or jail. Both settings must maintain tightly controlled security around the periphery of the facility and an internal vigilance for internal security concerns. However, CSH has an additional internal security overlay that requires an ongoing staff focus on surveillance, containment, clinical-supervision of interpersonal relationships, and an active support of a therapeutic "least restrictive treatment environment".

B. Staff Responsibility:

1. All employees that operate within the security setting of the facility are provided training and supervision to ensure competency and compliance with essential security policies and procedures.

2. Staff shall not violate therapeutic boundaries with Individuals.

3. Relationship security, a critical component in prevention of security breeches, involves monitoring all interactions for boundary problems that may manifest as individual exploitation, criminal activity and escape risks. All employees are responsible to support the hospital's relationship security program by being vigilant for, and to report, undesirable interpersonal relationships between staff or involving staff and Individuals.

4. All staff members are responsible for safe practices and adherence to CSH policy and procedures. To maintain control over contraband, staff is subject to search both randomly and for cause.

5. Staff shall not place themselves in situations where they are isolated from contact with or direct observation by other staff. All windows, including office doors, shall be left uncovered with exceptions requiring approval by the Executive Director. The immediate supervisor must approve activities calling for an employee to be in isolated situations with Individuals.

6. All staff and Individuals are assisted in maintaining the facility's norm of non-violence through processes that foster effective communication and pro-social conflict management.

7. Individual involvement in maintenance of security is encouraged and accomplished through working with the area specific staff, individual health and safety program and the effective use of therapeutic community meetings.

8. Effective care and treatment of forensic Individuals' calls for a balance between two forces typically referred to as "custody" and "care". It is a core CSH value that a positive treatment environment be maintained at all times within the facility. Barring emergent situations, routine custody or security routines will not interfere with the treatment milieu. Maintaining an effective balance between custody and care will be an ongoing focus of clinical and administrative staff.

9. It is essential that DPS and the clinical program staff work together to create and maintain a secure environment conducive to effective treatment and rehabilitation. DPS and clinical staff shall engage regularly in ongoing planning and evaluation of security procedures through daily one-to-one dialogue and in structured cross-departmental processes and functions. In an effort to also link security practices with a high degree of accountability tied to specific areas of expertise, DPS and clinical staff has been delegated primary responsibility for certain aspects of security.

    a. DPS will coordinate and control CDCR operations at CSH to ensure all operations are consistent with DMH policies, procedures, and all applicable special orders. CDCR, with augmentation by DPS, is assigned the primary responsibility for monitoring and controlling all pedestrian and vehicle traffic entering or exiting the hospital grounds and buildings within the specific security perimeter. DPS will conduct inspections, control procedures, and perform all law enforcement functions or other police/security related duties for the facility.

    b. The clinical program staff of the hospital have primary responsibility for the planning and management of the care, treatment, and activities of each Individual, and the ongoing moment-by-moment and day-to-day direction and control of the behavior of Individuals.

    c. The clinical staff and the DPS staff share many responsibilities in the day-to-day management of the internal security of the hospital. To foster communication and understanding relative to these over lapping functions, CSH has seen to it that whenever possible, DPS and clinical staff train together.

C. Criminal Activity:

1. Crime Defined: An act that is committed (or omitted) in violation of a law which forbids or commands it and for which punishment is imposed by a court of law upon conviction of said act.

    a. Any employee who witnesses or discovers what may be a crime, such as an assault, any security breeches, destruction of state property, discovery of drugs, illegal contraband or other possible crimes is required to:

i. Call for needed Medical and Police Services response.

ii. Provide needed assistance or medical attention as necessary.

iii. If DPS are not present, staff shall preserve the crime scene to the extent possible without compromising the health and welfare of any staff or Individual. Staff shall preserve the scene until relieved by DPS who will then take full control until the completion of the investigation.

2. Crime Scene Defined: The "crime scene" is the locale within the immediate vicinity of the occurrence wherein evidence may be found. Obviously, the perimeter of the crime scene will depend on the type and location of the crime.

3. Evidence Defined: Data presented to a court or jury in proof of the facts in issue and which may include the testimony of witnesses, records, documents, or objects such as blood samples, fingerprints, weapon/s, clothing, etc.

4. Primary precautions for preserving a crime scene/maintaining integrity of evidence are:

a. Do not move anything unless it is absolutely necessary, then only do so wearing latex gloves and leave a marking (pencil/ pen/ masking tape, etc) showing the original location;

b. to the extent possible, avoid contamination of evidence by smearing fingerprints, blood, etc – leave everything as you found it;

c. protect physical evidence from the elements using shading, tarps, etc when necessary to protect from strong wind, rain, etc;

d. maintain evidence in possession of the person who seized it until it can be handed over to police for processing;

e. do not cross-contaminate evidence (i.e. keep each piece of evidence separate from other evidence);

f. isolate witnesses from each other and other persons;

g. if a computer is part of a crime scene and no apparent attempt to destroy computer-based evidence has been observed, the computer should not be disturbed and the computer systems administration staff should be notified; however, if an apparent attempt to destroy or alter computer-based evidence has been observed (such as rapidly blinking hard drive access light), turn the computer off as quickly as possible and keep it safe from any unauthorized intervention.

D. Crime Scene Preservation By DPS Staff:

1. The first DPS Officer to arrive at the scene of a suspected crime or death is responsible for the ongoing control and protection of the scene. The primary concern will be for; preservation of life, scene integrity/ security, identification of witnesses and additional resources that may be required. The DPS Officer is to relay any immediate concerns and/ or needs to the Watch Sergeant. The DPS Officer will maintain control until properly relieved by the Senior Special Investigator/ designee or a DPS supervisor.

   a. Preservation of life will entail providing immediate medical attention to anyone connected to the crime scene who may have a life-threatening injury or illness. All precautions will be taken to ensure that the crime scene is neither disturbed nor contaminated if medical care is given at the scene or if the person is removed from the scene. When at all possible, without delaying lifesaving medical aid, photos will be taken of the injured party at the scene prior to being moved out to document their placement/ involvement within the crime scene.

   b. Scene Integrity/ Security will be established by setting a perimeter surrounding the incident area. The perimeter will be set beyond the immediate crime scene area and will be considered an outer perimeter. Normal activities may continue outside the perimeter, but may not infringe upon the vicinity of the crime scene. The immediate crime scene area may be cordoned off using barrier tape when necessary to restrict access to that area. Access to the crime scene is to be restricted to only those staff that have an intrinsic need to enter. A record is to be kept, documenting who is given access, when, and why. Additional staff may be recruited to assist in maintaining the crime scene's integrity.

   c. Identification of witness/es will include recording of identifying and contact information for both eyewitnesses and material witnesses. Unless impossible to do so, the witness/es will be separated in order to obtain independent statements/ information during interviews.

   d. Additional Resources will include, but not limited to; the use of other personnel to assist with perimeter and/ or crime scene security, medical staff to deliver medical services to those in need, transportation of injured to medical facilities, use of Public Information Officer, etc.

E. CSH will participate in DMH Security Audits as per Special Order 247.03.

A three-year state hospital security audit cycle began January 2005. For the first two years focused security audits will occur each calendar year followed by full security audits every third year.

1. Audit Tool:

   The state hospitals will be audited by use of the Long Term Care Services (LTCS) audit tool. The audit tool may be revised, as appropriate, with approval of the Executive Directors. The audit tool includes:

   a. Table of Contents;

   b. Introduction;

   c. Audit Scope and Methodology;

   d. Compliance Chart;

   e. Summary of Findings;

   f. Narrative;

   g. Special Orders: 202.02, 239.02, 240.01, 241.03, 242.01, 243.02, 244, 245.01, 246.01, 256, 315.05, 323.02, 326, 332.01, 327, 416.01, 903.05;

   h. Personnel component for Hospital Police Officers;

   i. Perimeter security components;

   j. Security awareness education plan component;

   k. Rating Sheets for each audit area.

2. Full State Hospital Security Audit:

   a. A full security audit encompasses all the audit areas identified in the audit tool. The areas are divided into three groups. The audits routinely take three days to complete, and include day and evening site work to observe and speak with staff. To facilitate this type of security audit the following will occur.

   b. The LTCS Chief of Hospital Security and Safety will lead the security audits. The Chief is responsible for scheduling the audit dates, making notifications and arrangements for the audits, facilitating the entrance and exit conferences, assigning duties to the audit team members, clarifying issues, answering questions, and developing and submitting a preliminary draft security audit report at the exit conference.

c. Each hospital will designate at least one employee to conduct security audits at state hospitals other than their respective hospital. The employees will work with site personnel and be responsible for an assigned audit group. Preferably, the designated employee(s) should have prior experience in conducting state hospital security audits, and be a member of their respective state hospital's internal security committee. The state hospitals are responsible for any costs incurred for their employees who participate in the security audits.

d. To facilitate the audit team, the state hospital audited will dedicate at least three site employees during the duration of the audit to assist the audit team members by securing requested documentation and to provide escort services.

e. In preparing for the audit, the Chief will make the following notifications and requests to the Executive Director when scheduling the audit:

   i. The dates of the security audit (minimum of three weeks in advance);

   ii. The names of the LTCS audit team members;

   iii. A copy of the audit tool;

   iv. A request for documents for each audit area;

   v. A contact person for administrative and technical support;

   vi. A request for office space, telephones, and other equipment, as needed;

   vii. A formal request to the Executive Director for an entrance and exit conference.

f. The Chief will provide the Executive Director a hard copy of a preliminary draft security audit report at the exit conference and accept any additional information and documents at that time. The preliminary draft security audit report will identify areas of compliance and areas in need of improvement. The Chief will review and make appropriate revisions to the preliminary draft security audit report and submit a final draft security audit report to the Executive Director within two weeks of the security audit.

g. The Executive Director will respond to the findings of the final draft security audit report by producing a detailed plan of correction for all areas that did not receive a compliance rating within thirty days and forward the plan to the Deputy Director, LTCS. Any other additional information regarding areas of disagreement or to identify a need for clarification may be submitted with the response.

h. The Deputy Director, in consult with the Chief, will review and evaluate the response to determine whether it meets the goals and objectives of the Special Orders and other audit areas, and make revisions to the final draft security audit report, as needed. The Executive Director will be notified regarding the acceptability of the response, and provided the opportunity to resubmit information concerning any part of the plan of correction that is not acceptable. Any revised plan of correction must be submitted within two weeks.

i. In accordance with the provisions in the plan of correction, the Chief may conduct follow-up compliance reviews to verify the plans have been implemented and are in compliance with the identified audited areas. The Chief will submit a follow-up report to the Deputy Director, LTCS, regarding the review and the Executive Director will be noticed, as well.

3. Focused State Hospital Security Audits:

a. On a two-year cycle, focused state hospital security audits will be conducted at each state hospital. These security audits are short in duration (one to two days) and focus on three or four security audit areas. To facilitate this type of security audit the following will occur.

i. Each state hospital will make available one employee who will work with the Chief to conduct the audits. Atascadero State Hospital or CSH will designate an employee to work with the Chief to audit Napa State Hospital and vice versa. Likewise, Metropolitan and Patton State Hospitals will assign personnel to conduct audits in the same manner. Personnel assigned to conduct the audits should have prior state hospital security audit experience and the LTCS Chief will participate in the selection of the employees. The state hospitals are responsible for costs incurred for their employees who participate in the security audits.

ii. The Chief is responsible for: notifying the state hospital of the security audit date(s), will work directly with the assigned state hospital employee to prepare for the audit, make needed arrangements, facilitate the entrance and exit meetings, and verbally provide preliminary findings of the security audit to the Executive Director.

iii. The security audits will be scheduled at least three weeks in advance; however, the audit areas will not be revealed until the team arrives. The state hospital scheduled for audit will dedicate at least one employee who will assist the audit team and provide escort. The state hospital will make arrangements for office space, telephones, and other necessary equipment to the audit team.

iv. Within one week of the completion of the security audit, the Chief will submit a final draft security audit report to the Executive Director. The report will identify areas of compliance as well as areas in need of improvement.

v. The Executive Director will submit a detailed plan of correction for all audited areas that need improvement within thirty (30) days of the receipt of the final draft security audit report. Clarifying information may be submitted with the response.

vi. The Deputy Director, in consult with the Chief, will review and evaluate the plan of correction, and make revisions to the final draft security audit report, if warranted. The Executive Director will be notified as to the acceptability of the response may submit additional information for consideration. Any revised plan of correction must be submitted within two weeks.

vii. The Chief may conduct follow-up compliance reviews at the state hospitals to determine if the plan of correction has been fully implemented and is in compliance with the audited areas. The Chief will submit a report to the Deputy Director, LTCS, regarding the follow-up reviews and the Executive Directors will also be noticed.

BEN MCLAIN
Executive Director (Acting)

Cross Reference(s):
A.D. No. 130 Facility Declaration
A.D. No. 150 Relationship Security: Safe Therapeutic Interactions