Records Procedures

802.1 PURPOSE AND SCOPE

This policy establishes the guidelines for the operational functions of the Department of State Hospitals (DSH) Office of Protective Services' (OPS) Records Group (Records). The policy addresses DSH file access and internal requests for OPS case reports.

802.2 POLICY

It is the policy of DSH to maintain DSH records securely, professionally and efficiently.

802.3 RESPONSIBILITIES

802.3.1 RECORDS MANAGER

The Hospital Police Chief shall appoint and delegate certain responsibilities to an OPS Records Manager. The Records Manager shall be directly responsible to the Hospital Police Chief or designee.

The responsibilities of the Records Manager include, but are not limited to:

(a) Overseeing the efficient and effective operation of Records.

(b) Scheduling and maintaining Records time records.

(c) Supervising, training and evaluating Records staff.

(d) Maintaining and updating a Records procedure manual.

(e) Ensuring compliance with established DSH and OPS policies and procedures.

(f) Supervising the access, use and release of protected information. (See the Protected Information Policy.).

(g) Establishing security and access protocols for case reports designated as sensitive, where additional restrictions to access have been implemented. Sensitive reports may include, but are not limited to:

1. Homicides.
2. Cases involving DSH employees or public officials.

3. Any case where restricted access is required or prudent.

802.3.2 RECORDS

The responsibilities of Records include, but are not limited to:

(a) Maintaining a records management system for case reports.

1. The records management system should include a process for numbering, identifying, tracking and retrieving case reports.

(b) Entering case report information into the records management system.

1. Modification of case reports shall only be made when authorized by a supervisor.

(c) Providing DSH employees access to case reports when needed for investigation or court proceedings.

(d) Complying with federal, state and local laws and regulations regarding reporting requirements of crime statistics, as well as those addressing patient and employee privacy. This includes reporting statistical data to the California Department of Justice (DOJ) for:

1. All officer-involved shootings and incidents involving use of force resulting in serious bodily injury (Gov. Code § 12525.2).
2. Suspected hate crimes (Pen. Code § 13023).
3. Complaints of racial bias against officers (Pen. code § 13012; Pen. Code § 13020).
4. Civilian complaints made against officers (Pen. Code § 832.5; Pen. Code § 13012).
5. Stop data required by Government Code section 12525.5 and California Code of Regulations title 11 section 999.226.
    i. The reported information must not contain personally identifiable information of the person stopped or other information exempt from disclosure pursuant to Government Code section 12525.5 (Cal. Code Regs., tit.11 § 999.228).

(e) Maintaining compliance with federal, state and local regulations regarding criminal history reports and auditing, as well as patient and employee privacy.

(f) Identifying missing case reports and notifying the responsible employee's supervisor.

(g) Updating the Automated Firearms System to reflect any firearms relinquished to the OPS and the subsequent disposition to the DOJ pursuant to Penal Code section 34010. (Pen. Code § 29810).

(h) Entering into the Automated Firearms System information about each firearm that has been reported stolen, lost, found, recovered, held for safekeeping, or under observation within seven calendar days of the precipitating event.

(Pen. Code § 11108.2.)

(i) Maintaining compliance with the state and DOJ reporting requirements regarding the number of transfers of individuals to immigration authorities and offenses that allowed for the transfers (Gov. Code § 7284.6, subd (c)(2)).

(j) Contacting the privacy officer at the appropriate DSH location, or DSH Legal Division in Sacramento, as soon as it is suspected that patient or employee information has been improperly released to an unauthorized party.

802.3.3 RECORDS PROCEDURE MANUAL

The Records Manager should establish procedures that address:

(a) Identifying by name persons in reports.

(b) Classifying reports by type of incident or crime.

(c) Tracking reports through the approval process.

(d) Assigning alpha-numerical records to all arrest records.

(e) Managing a warrant and wanted persons file.

802.4 DETERMINATION OF FACTUAL INNOCENCE

In any case where a person has been arrested by officers of OPS and no accusatory pleading has been filed, the person arrested may petition OPS to destroy the related arrest records. Petitions should be forwarded to the Hospital Police Chief or designee. The Hospital Police Chief or designee should promptly contact the prosecuting attorney and request a written opinion as to whether the petitioner is factually innocent of the charges. (Pen. Code, § 851.8). Factual innocence means the accused person did not commit the crime.

Upon receipt of a written opinion from the prosecuting attorney affirming factual innocence, the Hospital Police Chief or designee should forward the petition to Investigations for review. After such review, the Investigations supervisor and the Hospital Police Chief or designee shall decide whether a finding of factual innocence is appropriate.

Upon determination that a finding of factual innocence is appropriate, the Hospital Police Chief or designee shall ensure that the arrest record and petition are sealed for later destruction and the required notifications are made to the California Department of Justice and other law enforcement agencies. (Pen. Code, § 851.8.)

The Hospital Police Chief or designee should respond to a petition with the OPS decision within 45 days of receipt. Responses should include only the decision of OPS, not an explanation of the analysis leading to the decision.

802.5 ARREST WITHOUT FILING OF ACCUSATORY PLEADING

The Hospital Police Chief or authorized designee should ensure a process is in place for when an individual is arrested and released and no accusatory pleading is filed so that the following occurs (Pen. Code §§ 849.5, 851.6):

(a) The individual is issued a certificate describing the action as a detention.

(b) All references to an arrest are deleted from the arrest records of DSH and the record reflects only a detention.

(c) The Bureau of Criminal Identification and Investigation of the Department of Justice is notified.

802.6 FILE ACCESS AND SECURITY

The security of files in Records must be a high priority and shall be maintained as mandated by state or federal law. All case reports including, but not limited to, initial, supplemental, follow-up, evidence and any other reports related to a DSH case, including field interview (FI) cards, criminal history records and publicly accessible logs, shall be maintained in a secure area within Records, accessible only by authorized Records employees. Access to case reports or files when Records staff is not available may be obtained through the Watch Commander.

Records will also maintain a secure file for case reports deemed by the Hospital Police Chief as sensitive or otherwise requiring extraordinary access restrictions.

802.7 ORIGINAL CASE REPORTS

Generally, original case reports shall not be removed from Records. Should an original case report be needed for any reason, the requesting DSH employee shall first obtain authorization from the Records Manager. All original case reports removed from Records shall be recorded on a designated report check-out log, which shall be the only authorized manner by which an original case report may be removed from Records.

All original case reports to be removed from the Records shall be photocopied and the photocopy retained in the file location of the original case report until the original is returned to Records. The photocopied report shall be shredded upon return of the original report to the file.

802.8 CONFIDENTIALITY

Records staff has access to information that may be confidential or sensitive in nature. Records staff shall not access, view or distribute, or allow anyone else to access, view or distribute any record, file or report, whether in hard copy or electronic file format, or any other confidential, protected or sensitive information except in accordance with the Records Maintenance and Release and Protected Information policies and the Records procedure manual.