SECTION - MEDICAL/NURSING SERVICES
ADMINISTRATIVE DIRECTIVE NO 584
(Replaces A.D. No. 584 dated 2/14/07)

Effective Date: March 8, 2007

SUBJECT: HIPAA HEALTH INFORMATION PRIVACY AND SECURITY PROGRAM

I. PURPOSE

A. The purpose of a health information privacy and security program is to ensure the continued integrity of confidential health information, while communicating both internally and with our external customers. Protection of individually identifiable health information may include reinforcing administrative directives, developing physical safeguards and technical security practices, soliciting the support of our business associates, and training our hospital workforce as to their responsibilities for keeping health information confidential.

B. The limitations of implementing the Privacy Rule in a psychiatric forensic facility are recognized by the hospital. The need for physical safety of both Individuals and staff may override the individual patient's right to health information privacy. The hospital has developed a multilevel process for evaluating all Protected Health Information (PHI) concerns in order to acknowledge all patient confidentiality requests, identify patient treatment issues, and support a safe and secure facility.

II. AUTHORITY

Department of Mental Health (DMH) Special Orders 261 and 512; Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule; 45 CFR 160 and 164; Information Practices Act 1977 (California Civil Code 1798); Lanterman-Petris-Short Act (California Welfare and Institutions Code 5328).

III. POLICY

It is the policy of Coalinga State Hospital (CSH) to clearly define and adhere to a procedure to protect the privacy and security of the medical record.

IV. METHOD

A. Administrative Responsibility:

1. The Executive Director will appoint a Privacy Officer and a Security Officer. These individuals will have the responsibility for directing, enforcing, and managing the development and implementation of hospital-wide activities related to the privacy and security of protected health information. These individuals must be knowledgeable of hospital operations and state/federal laws as they relate to protection of health information in its many forms (e.g. verbal communication, paper medical record, electronic transmission of data). The Privacy Officer and the Security Officer will be entrusted with the authority and executive backing to accomplish their tasks. Duty Statements for these individuals will reflect their official designations.

2. The Privacy Officer will chair a standing committee to be known as the "Protected Health Information Team" (A.D. No. 278) whose purpose will be to evaluate all health information privacy complaints and all patient requests for amendment to the medical record. The Privacy Officer will be responsible for assuring that efficient processes exist for (1) documenting all written privacy-related complaints, suggestions, or requests; (2) directing resolution and follow-up as necessary, and (3) reporting the status of the privacy issues/concerns to the Executive Director. These processes will be periodically monitored and audited for compliance by the Performance Improvement Coordinator.

3. The Security Officer will be responsible for ensuring the appropriate access to and protection of electronic protected health information at CSH. He/she will act as the internal information security consultant to the hospital and report the status of information security issues/concerns to the Executive Director. His/her duties will include the development and monitoring of administrative procedures, physical safeguards, technical services, and technical mechanisms to support compliance of state and federal information security laws.

4. The Health Information Management Department (HIMD) Director shall serve as the Access Officer, and be responsible for maintaining the accuracy and integrity of patient medical records. He/she will respond to written requests/authorizations for medical record information, oversee release of medical information, and schedule patient and outside reviewer access to the medical records. He/she will be an integral part of the HIPAA Team in consultation with the assigned Privacy and Security Officers.

B. Workforce Confidentiality/Training:

1. Employees, volunteers, students, interns, and contractors have the responsibility for protecting the patient health information to which they have access during the performance of their duties. Training on privacy and confidentiality will be provided during New Employee Orientation, work site orientation, and as required by hospital training category.

2. Each employee will be required to review the HIPAA Health Information Privacy and Security Program administrative directive and sign a statement of understanding to be kept in his or her Personnel file.

C. Addressing Privacy Issues with Business Associates:

1. CSH, as a health care provider, is considered a "covered entity" according to federal privacy laws. Those individuals/organizations with whom we contract services that use or disclose patient health information as part of their job will be identified as our "Business Associates," and tracked for confidentiality clauses (Exhibit E) in their business contracts.

2. These individuals/organizations will be, through an amendment to their written contracts, required to maintain confidentiality of our patient health information by agreeing to not violate federal privacy use and disclosure regulations. Business associates may use or disclose PHI if they give reasonable assurances that they will appropriately safeguard the information. Violations of those assurances will place the business associate in non-compliance with the Privacy Rule. The hospital is not required to monitor or oversee how the business associates carry out their privacy and security safeguards, nor are they liable for the actions of the business associates. However, the hospital is responsible for taking reasonable steps to cure privacy breaches or end violations and, if unsuccessful, terminate the contract with the business associate.

D. Uses and Disclosures of Patient Health Information:

1. As a health care provider, the hospital is allowed to use and/or disclose individually identifiable health information for treatment, payment, and health care operations.

2. In addition, the hospital can use and/or disclose information with a written authorization from the Individual, or as required/allowed by law.

E. News Media Requests:

1. Information requests from the news media regarding significant events regarding Individuals receiving services shall be directed to the Public Information Officer (PIO).

2. The PIO shall consider all requests from the media as public information requests and shall limit the release of information to that which is detailed in Special Order 261.

F. Privacy and Security Safeguards:

1. Protected health information (written, verbal, or electronic) must be administratively, technically, and physically protected to ensure confidentiality.

2. The hospital is responsible for reasonably safeguarding protected health information from any intentional or unintentional use of disclosure that is in violation of the standards.

3. The hospital is responsible for reasonably safeguarding protected health information to limit incidental uses and disclosures.

G. Privacy and Security Sanctions:

1. Acts arising from carelessness or failure to follow procedures include but are not limited to the following examples:

a. Failure to sign off properly from a workstation.

b. Leaving medical records or a copy of PHI or other confidential information in a non-secure area.

c. E-mailing a file that includes PHI or other confidential information to the wrong person.

d. Faxing PHI or confidential information to the wrong fax number.

e. Dictating or discussing PHI or other confidential information in a non-secure area (lobby, hallway, cafeteria, and elevator).

f. Improper disposal of PHI or other confidential information.

g. Not properly verifying individuals prior to releasing PHI or other confidential information by phone, in person or in writing.

h. Failure to document disclosures properly on the Patient Record Review Form or the Disclosure Tracking System.

i. Failure to take reasonable precautions to prevent incidental disclosure of PHI or other confidential information.

j. Corrective actions may include but are not limited to:

i. Revising policies and procedures.

ii. Revising training procedures.

iii. Additional training to employees with documentation.

iv. Verbal instruction with documentation.

2. Acts arising from purposeful failure to follow procedures include but are not limited to the following examples:

   a. Sharing a password with another co-worker or using another co-worker's password.

   b. Intentionally accessing records containing PHI or other confidential information without proper authorization.

   c. Repeated violations due to carelessness.

   d. Neglecting to self-report incidents.

   e. Corrective actions may include, but are not limited to:

      i. Information counseling.

      ii. Formal corrective interview.

      iii. Adverse action including: Official Letter of Reprimand, reduction in salary, suspension without pay, demotion, and mandatory transfer or dismissal from state service.

      iv. Revision of training procedures.

3. Acts arising from purposeful, blatant misuses of PHI or other confidential information include but are not limited to the following examples:

   a. Accessing or allowing access to PHI or other confidential information for personal gain or malicious intent.

   b. Intentional tampering with or unauthorized destruction of PHI or other confidential information.

   c. Deliberate acts that adversely affect the confidentiality or integrity of PHI or other confidential information.

   d. Repeated violations of previous levels.

   e. Corrective actions may include, but are not limited to:

      i. Adverse action including an Official Letter of Reprimand;

      ii. Reduction in salary;

      iii. Suspension without pay;

iv. Demotion;

v. Mandatory transfer;

vi. Dismissal from state service.

H. Patients' Information Privacy Rights:

1. All Individuals will be provided with a copy of the "Department of Mental Health Notice of Privacy Practices" upon admission to the hospital. A reasonable attempt will be made to have the Individual sign an acknowledgment of receipt, which will be placed in the Consent section of their medical record. If the Individual refuses to sign the acknowledgment, the acknowledgment will be marked as refused, dated, signed by the employee, and filed in the medical record in the Consent section. The hospital will not use or disclose PHI in a manner inconsistent with the Notice of Privacy Practices.

2. Individuals have the right to request a review and have copies of their designated medical record. The Individual may be billed for the copies.

3. Individuals have the right to request an amendment to their medical record. Requests will be referred to the Protected Health Information Team (PHIT) to review, respond, and track all disagreements of denials.

4. Individuals have the right to receive an accounting of their PHI disclosures. The hospital must track all PHI that goes to individuals or organizations outside of CSH who do not have an Individual's written authorization or who are not directly involved in the Individual's treatment, payment, or hospital operations. There will be a fee for processing this list if requested more than once every 12 months.

5. Individuals have the right to request restrictions or limitations on their health information that is used for treatment, payment, or health care operations. Requests are to be submitted in writing to the Privacy Officer and include what information is to be limited, whether it applies to use and/or disclosures, and to whom the limit is to apply. Agreed upon restrictions will be followed, unless the information is needed to provide the Individual with emergency treatment. The hospital is not required to agree to the request.

6. Individuals have the right to request that the hospital communicate with them about medical matters in a confidential manner. Requests are to be in writing to the Privacy Officer and specify how the information is to be communicated. All reasonable requests will be accommodated.

I. Health Information Privacy Complaint Process:

1. The Information Privacy Official will also act as the Information Privacy Complaint Officer for all issues relating to protected health information. The Privacy Complaint Officer will have access to employee and patient records in order to monitor compliance with the privacy laws and will have the authority to investigate all appropriate privacy complaints.

2. The Privacy Complaint Officer can recommend business process changes, negotiate to resolve complaints caused by inappropriate business practices, and suggest actions to mitigate harmful effects resulting from Privacy Act violations. It will be the responsibility of the Privacy Officer to monitor all privacy complaints and compliance with federal and state privacy laws.

J. Privacy Violation, Mitigation and Sanctions:

1. The Federal Privacy Rule requires that CSH have and apply appropriate sanctions against members of its workforce who fail to comply with the hospital privacy policies and procedures.

2. Civil and/or criminal penalties are potential consequences of information privacy infractions. The infractions may include both the release of health information to inappropriate parties and the failure to adequately protect the information from being released. Knowingly releasing patient information, gaining access to information under false pretenses, and releasing information with intent to sell or cause harm are all grounds for criminal penalties.

3. Members of the workforce are to be given clear expectation of their responsibility in complying with the privacy laws during hospital orientation and annually, through the Annual Review Training (ART).

4. Disciplinary action will follow the state process of prevention, corrective action, and adverse action as determined by the employee's supervisor and the Privacy Officer. The severity of the sanction will depend on the degree of the violation, and the degree to which it could be mitigated.

5. Those members of the workforce who are not employees (e.g. interns, students, volunteers, or contractors), will be disciplined through their appropriate supervisors. Privacy breaches through business associates will be considered a violation of the contract agreement.

6. The Privacy Officer shall monitor documentation of the sanctions applied.

7. Complaints, whistleblowers, and privacy investigation activities shall be exempt from sanctions when bringing noncompliance to the attention of the hospital. The hospital will not be violating the Privacy Rule if the member of the workforce or business associate discloses PHI, provided that they acted in good faith in that the violation potentially endangered an Individual, a worker, or the public; and the disclosure was to a health oversight agency authorized to investigate the allegations or to an attorney retained by the whistleblower.

8. It is the responsibility of the hospital to prevent workforce members from taking intimidating, threatening, coercive, discriminatory, or other retaliatory actions against individuals who file complaints.

9. The hospital will not violate the Privacy Rule if a member of the workforce who is a victim of a criminal act discloses PHI to law enforcement official, provided that the information was about the suspect and the PHI was limited to the identification and location of the suspect (45 CFR 164.512(f)).

V. DOCUMENTATION AND COMPLIANCE ACTIVITIES

A. HIMD:

1. Documentation Retention: All documentation pertaining to correction, amendment/addendum, and accounting of disclosure are maintained by HIMD for a minimum of seven years after the last contact with the Individual.

2. All requests for amendments, addendums and disclosures are logged and tracked in HIMD, and forwarded to the PHI Committee for action.

3. The PHI Team, chaired by the Privacy Officer, reviews HIPAA-related requests/complaints and participates in the resolution of it. All privacy complaints will be maintained by the Privacy Officer for a minimum of seven years after the last contact with the Individual.

4. The Patient Input Section of the medical record is used exclusively for filing and linking of processed HIPAA documents.

5. Accounting of Disclosures: When PHI is released to third parties without patient authorization (e.g. court order, public health), the disclosure details are entered into a hospital database. Database information is retained in order to respond to future patient inquiries.

6. Audits are conducted no less than annually to measure compliance with the requirement that Individuals receive the Notice of Privacy Practices upon admission.

B. The PHI Committee shall select audit teams to perform privacy and security inspections on a quarterly basis.

C. Patient Care Policy Committee:

HIPAA Administrative Directives are reviewed/updated no less than annually.

D. Accounting Department:

1. The Standard Contract Process includes determination as to whether a HIPAA Business Associate (BA) clause is required.

2. Identified HIPAA BA contracts are audited no less than annually for the presence of appropriate HIPAA language.

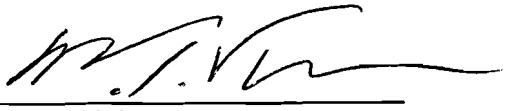
E. Standards Compliance:

1. The Information Management chapter incorporates HIPAA requirements into the JCAHO survey readiness process.

2. The Patients' Rights Advocate, PHIT, or the HIMD Director shall notify the Director of Standards Compliance when a HIPAA violation has occurred.

F. Training:

Mandatory training on HIPAA is provided through New Employee/Student/ Contractor Orientation, worksite orientation, and annually as part of the ART.



W. T. VOSS
Executive Director

Cross-reference(s):
A.D. No. 154 Public Relations
A.D. No. 278 Protected Health Information Committee
A.D. No. 580 Patient Medical Records: Confidentiality and Information Release, Maintenance, Retention, and Disposition
A.D. No. 581 HIPAA Patients' Access to the Medical Record
A.D. No. 583 HIPAA Protected Health Information – Use and Disclosure
A.D. No. 585 HIPAA Protected Health Information – Amendment or Correction Process
A.D. No. 586 Medical Record Charts
A.D. No. 587 Health Information Privacy Complaint Process
A.D. No. 722 Telecommunication
Special Order 261 Release of Information to the News Media Regarding Significant Events Concerning Individuals Served at State Hospitals and Psychiatric Programs