

CALIFORNIA DEPARTMENT OF CORRECTIONS AND REHABILITATION
CALIFORNIA CORRECTIONAL HEALTH CARE SERVICES
Health Care Department Operations Manual

2.3.2 Security and Privacy

(a) Policy

California Correctional Health Care Services (CCHCS) Health Information Management (HIM) shall adhere to established rules, guidelines, and statutes that protect patient privacy, confidentiality, security, access to, use, and disclosure of Protected Health Information (PHI). HIM, Health Records, and Information Technology Units shall ensure:

- (1) The use of appropriate technical safeguards, as stated in 45 Code of Federal Regulations Part 164, Subpart C, to restrict access to, protect the integrity of, and guard against the unauthorized access to electronic PHI.
- (2) Any tampering of PHI is identified and reported, as appropriate.
- (3) Availability of health information is readily accessible to the extent possible.
- (4) Capability of storing information pursuant to retention requirements.
- (5) Availability of backup and restore operation.
- (6) Management review of security periodically for necessary changes as a result of technology evolution.
- (7) Periodic risk assessments conducted by management in accordance with State Administrative Manual, Section 5305.6, Risk Management, to ascertain the threats and vulnerabilities that impact CCHCS and HIM assets, and implement appropriate mitigations.

(b) Purpose

To ensure protection of patient, privacy, security, access to, use, and disclosure of PHI.

(c) Policy Responsibility

- (1) The Chief Executive Officer, or designee, Health Record Technician III (HRT III), and Health Record Technician II (HRT II) of each institution are responsible for the implementation, monitoring, and evaluation of this policy.
- (2) The CCHCS Information Security Officer shall validate the security component for access to electronically stored PHI.

(d) Procedure Overview

CCHCS HIM shall ensure all employees are informed of and follow established rules, guidelines, and statutes that protect patient privacy, security, access to, use, and disclosure of PHI. As new technologies evolve with the use of computerized patient health records, HIM staff shall implement and reinforce procedures for authorizing access to PHI.

(e) Procedure Responsibility

Under the direction of the Deputy Director, Medical Services, HIM Headquarters, Institution Health Records, and Health Record Center (HRC) staff are responsible for the oversight, implementation, monitoring and evaluation of this procedure.

(f) Procedure

(1) PHI Identifiers

Any of the following personal data identifiers, used in combination with a medical condition, becomes PHI and shall not be disclosed without proper authorization or approval:

- (A) Names.
- (B) All geographic subdivisions smaller than a State including street address, city, county, precinct, zip code, and their equivalent geocodes. However, the initial three digits of a zip code may remain on the information if, according to current publicly-available data from the Bureau of the Census, the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and the initial three digits for all such geographic unit containing 20,000 or fewer people is changed to 000.
- (C) All elements of dates (except year) directly relating to the patient including birth date, dates of admission and discharge from a health care facility, and date of death. For persons age 90 and older, all elements of dates (including year) that would indicate such age must be removed, except that such ages and elements may be aggregated into a single category of "age 90 and older."
- (D) Telephone numbers.
- (E) Fax numbers.
- (F) Electronic mail addresses.
- (G) Social security numbers.
- (H) Health record numbers.

CALIFORNIA DEPARTMENT OF CORRECTIONS AND REHABILITATION
CALIFORNIA CORRECTIONAL HEALTH CARE SERVICES
Health Care Department Operations Manual

- (I) Health plan beneficiary numbers.
- (J) Account numbers.
- (K) Certificate or license numbers.
- (L) Vehicle identifiers and serial numbers including license plate numbers.
- (M) Device identifiers and serial numbers.
- (N) Web Universal Resource Locators.
- (O) Internet Protocol address numbers.
- (P) Biometric identifiers including fingerprints and voiceprints.
- (Q) Full face photographic images and any comparable images.
- (R) Any other unique identifying number, characteristic, or code.

(2) Accountability

- (A) All CCHCS/California Department of Corrections and Rehabilitation (CDCR) health care employees shall ensure PHI is covered or unable to be viewed at all times when information is not in use.
- (B) All computerized systems shall be protected with a unique user ID and a complex password.

(3) Backup and Storage of PHI

- (A) All CCHCS/CDCR health care employees shall ensure that any tampering of PHI is identified and reported to the Information Security Officer.
- (B) HIM, Health Records, and Information Technology Units shall ensure:
 1. The use of appropriate technical safeguards, as stated in 45 Code of Federal Regulations Part 164, Subpart C, to restrict access to, protect the integrity of, and guard against the unauthorized access to electronic PHI.
 2. Any tampering of PHI is identified and reported, as appropriate.
 3. Availability of health information is readily accessible to the extent possible.
 4. Capability of storing information pursuant to retention requirements.
 5. Availability of backup and restore operation.
 6. Management review of security periodically for necessary changes as a result of technology evolution.
 7. Periodic risk assessments conducted by management in accordance with State Administrative Manual, Section 5305.6, Risk Management, to ascertain the threats and vulnerabilities that impact CCHCS and HIM assets, and implement appropriate mitigations.

References

- Code of Federal Regulations, Title 45, Subtitle A, Chapter A, Subchapter C, Part 164, Subpart C, Security Standards for the Protection of Electronic Protected Health Information
- Code of Federal Regulations, Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- Code of Federal Regulations, Health Insurance Portability and Accountability Act of 1996, Summary of HIPAA Privacy Rules
- Code of Federal Regulations, Title 45, Subtitle A, Chapter A, Subchapter C, Part 164, Subpart E, Section 164.520, Notice of Privacy Practices for Protected Health Information
- California Civil Code, Division 1, Part 2.6, Confidentiality of Medical Information Act
- California Health and Safety Code, Division 2, Chapter 2, Article 3, Sections 1275-1289.5
- State Administrative Manual, Section 5305.6, Risk Management
- American Health Information Management Association, *Documentation for Ambulatory Care* (Revised ed. 2001)
- Health Care Department Operations Manual, Chapter 2, Article 2, Confidentiality and Privacy

Revision History

Effective: 01/2002

Revised: 02/2017