2.2.11 Privacy Incident and Potential Breach Reporting and Case Workflow

(a) Policy

California Correctional Health Care Services (CCHCS) shall identify, investigate, and mitigate potentially inappropriate access, use, or disclosures of Protected Health Information (PHI), Personally Identifiable Information (PII), and High-Risk Confidential Information (HRCI); provide notices when necessary to those affected and report breaches to the department's oversight agencies as required by federal and state law.

(b) Purpose

To provide guidance on reporting incidents and potential breaches and ensure CCHCS Privacy Office (PO) conducts mitigation efforts in compliance with federal and state law.

(c) Responsibility

(1) Oversight responsibility of the PO shall be vested in the Privacy Officer. The Privacy Officer shall oversee compliance with privacy policies and federal and state privacy laws and assist CCHCS in reporting the potentially inappropriate collection, access, use, or disclosure of PHI, PII, or HRCI under applicable laws, rules, and the California Department of Corrections and Rehabilitation (CDCR), Health Care Department Operations Manual (HCDOM).

(2) Incidents originating from CDCR activities including but not limited, to the CDCR Undersecretaries and offices that report to the CDCR Secretary, shall be referred to the CDCR Privacy Officer for fact-finding, analysis, intake, and response, except for those currently delegated to the CCHCS PO.

(3) For incidents involving CDCR and CCHCS, both entities shall coordinate fact-finding, analysis, intake, and response.

(d) Federal and CDCR Definitions

(1) PHI, PII, and HRCI

(A) **PHI – Protected Health Information** including all individually identifiable health information, mental health, dental, demographic data, medical histories, test results, insurance, and other information used to identify a patient, provide health care services or health care coverage held or disclosed in any form, whether electronic, paper, verbal or other media.

(B) **PII – Personally Identifiable Information** identifies or describes an individual, i.e., name, date of birth, address, social security number, etc**.,** held or disclosed in any form, whether electronic, paper, verbal or other media.

(C) **HRCI – High Risk Confidential Information** contains sensitive data that, if disclosed, could potentially cause harm to an individual, as identified in the CDCR Department Operations Manual (DOM).

(2) Privacy Incident or Breach

A privacy incident is anything considered or presumed to be a potential unlawful collection, access, use, or disclosure of PHI, PII, or HRCI. A privacy breach is determined after confirmation that an incident of unlawful collection, access, use, or disclosure of PHI, PII, or HRCI has occurred. The PO workforce reviews and conducts fact-finding for all incidents to determine if the incident resulted in a breach of protected information.

(e) Procedures

(1) Privacy Incident and Potential Breach Reporting

CCHCS workforce shall immediately report all privacy incidents or potential breaches to the CCHCS Information Security Office (ISO). All details shall be documented on the CCHCS Information Security Incident Report (ISIR) found on Lifeline, under Information Technology. CCHCS workforce shall ensure that the instructions listed on the ISIR are followed. The ISIR shall be emailed to the ISO who shall review the ISIRs, conduct an initial assessment, and assign a case number. The ISO shall forward any ISIR that documents incidents or potential breaches involving PHI, PII, or HRCI to the PO email box at CCHCSPrivacyOffice@cdcr.ca.gov.

(A) Incidents originating from CDCR shall be reported to the CDCR Privacy Officer.

(B) For incidents involving CDCR and CCHCS, both entities shall coordinate fact-finding, analysis, intake, and response.

(C) CCHCS workforce shall submit ISIRs documenting privacy incidents or potential breaches in plain language and meet the following reporting requirements if the information is available at the time the notice is provided:

1. The name and contact information of the reporting individual
2. A list of the types of confidential information reasonably believed to be the subject of an incident or

potential breach
3. The date or estimated date range within which the incident occurred
4. The incident or potential breach date of discovery and the date of the notice
5. Whether the notification was delayed because of a law enforcement investigation
6. A general description of the incident or potential breach
7. CCHCS program or unit related actions to gathering facts and investigating the incident or breach
8. Efforts to mitigate harm and protect against further incidents or breaches
9. Number of patients or individuals whose information was disclosed and number of individuals who received the protected information
10. Any additional steps individuals should take to protect themselves from potential harm

(2) Privacy Office ISIR Processing –Tracking Solution

(A) The PO workforce shall monitor the PO general mailbox daily. When a new ISIR is received from CCHCS ISO, the PO workforce shall screen the document within 24 business hours, adding the case number and incident details in the PO incident tracking solution.

(B) The case shall be promptly assigned, and the PO workforce shall request backup information from the individual who submitted the report. Others may be asked for information when needed. The assigned PO workforce shall conduct fact-finding using all available sources.

(C) When the fact-finding is complete, all relative information shall be documented in the risk assessment analysis, including the root cause, potential harm, and mitigation efforts. Once the risk assessment analysis is complete, the PO workforce shall have obtained sufficient case information to determine whether a breach notification will be issued.

(D) The PO workforce shall create a new case file to maintain all related information.

(E) The information maintained in the PO tracking solution shall be utilized for regular review of system activity, such as audit logs, incident tracking reports and sharing threat information with the California Department of Technology via direct electronic means. The information shall also be available for risk analysis or assessment which shall include (at a minimum) assignment of responsibilities for risk assessment, including appropriate participation of executive, technical and program management.

(3) Privacy Office Incident and Breach Tracking – Case File

The following case-specific information shall be provided and maintained in the PO case file:

(A) Initial details, including names of individuals involved, dates, and a description of incident or breach

(B) Pre-screening information

(C) How the incident or breach occurred

(D) Accounting of disclosure components

(E) Fact-finding and mitigation efforts and outcome

(F) Risk assessment

(G) Breach notice information

(H) Mandated reporting dates and information for oversight agencies

(I) Workforce training history and corrective action efforts

(4) Privacy Office Recovery and Destruction of Information Unlawfully or Improperly Disclosed

(A) The PO workforce shall work with those involved to immediately recover the original information or obtain written verification that the data in all media types have been properly destroyed.

(B) The ISIR, risk assessment, and breach notice incident-tracking log shall document mitigation efforts, mitigation outcomes, attestation, and affirmation of unresolved risks.

(C) Once the information (i.e., hard copies, electronic and portable media) is recovered, it shall be secured in an approved locked shred container, shredded, deleted, or disposed of according to the ISO process for electronic destruction.

(D) Privacy Office staff shall document all efforts and outcomes and include the information in the ISIR, breach notice, case file, tracking log, and risk assessment.

(5) Privacy Office Incident or Breach Fact-Finding and Risk Assessment and Analysis

(A) The PO workforce shall work with the individual(s) who reported the incident and with those who improperly received the potentially inappropriate information to conduct fact-finding and mitigation efforts. PO workforce

shall collaborate with Information Technology, Health Information Management, program unit managers, and others to recover, correct, or resolve the incident. PO workforce shall document all actions, progress, and outcomes in the PO tracking solution and case file, including documentation of the following information in the risk assessment to evaluate further the risk of harm to those involved:

1. The nature and extent of the information involved, including the types of identifiers and the likelihood of re-identification.
2. The person or entity who used the protected information or to whom the disclosure was made.
3. Whether the information was acquired or viewed.
4. Whether a purge of the emails was requested and completed.
5. The number of individuals affected.
6. The extent to which the risk of harm to the individual has been mitigated.
7. The root cause of the breach.
8. Corrective actions to mitigate future incidents.
9. Details describing the use of incident or breach information.
10. Description of the CCHCS risk management activities to assist in identifying additional threats and vulnerabilities.
11. Documented activities working with business associates or contractors to determine involvement in a breach and include any associated efforts to mitigate and prevent future occurrence.
12. All impermissible disclosures must be recorded in the state entity's Accounting of Disclosure tracking log. The log must record, at a minimum, the date of disclosure, name and address of the entity who received the health information, a brief description of the information disclosed, and a brief description of the reason for the disclosure.

(B) The Privacy Officer, or designee, shall review the content provided in the risk assessment to determine if additional information or corrective action(s) are needed or approve the completed risk assessment.

1. The Privacy Officer shall coordinate as required with the ISO to complete the risk assessment.

(6) Breach Reporting Responsibilities to Oversight Agencies

When determined that a breach has occurred, the Information Security Officer shall report the breach to the Office of Information Security (OIS) California Compliance Security Incident Reporting System (CAL CSIRS) and the California Highway Patrol as required.

(A) When the breach occurs at a clinic, health facility, home health agency, or hospice licensed by the California Department of Public Health (CDPH), CCHCS workforce shall immediately report the incident or breach. The breach reporting requirements are outlined in California Code of Regulations, Title 22, Section 79902, at the following link: Breach Reporting for Licensed Facilities. If you have further questions, you may contact the local Correctional Health Services Administrator or the Joint Commission Accreditation and Licensing Compliance Unit in Corrections Services.

(B) Business associates, or contracted entities shall immediately notify the CCHCS ISO when there has been an incident or potential breach of health information at the CCHCS Information Security Office; email: CCHCS-ISO@cdcr.ca.gov; or by Phone: (916) 691-3243. If the incident occurs after business hours or on a weekend or holiday and involves electronic PHI, notification shall be provided by calling the CCHCS ITSD Solution Center at 1-888-735-3470. Upon receipt of an ISIR involving a business associate, the Privacy Office workforce shall contact the entity responsible for monitoring the business associate agreement, and contact the business associate to begin mitigation efforts. The PO shall maintain a current list of all contracts, Data Sharing Agreements, or Memorandum of Understandings containing Business Associate Agreements and generate a current list based on contracting unit updates upon request. Refer to the HCDOM, Section 2.2.9, Business Associate Use and Disclosure of Protected Health Information.

(C) When A Breach Affects More than 500 Individuals

The PO workforce shall notify the Center for Data Insights and Innovation (CDII) at CDIIPrivacyOffice@chhs.ca.gov.

1. When the PO workforce provides notice to those affected by a breach involving 500 or more individuals, they shall also consecutively notify the Department of Health and Human Services (HHS) on the Breach Reporting form located on the HHS website at https://www.hhs.gov.

2. See further instruction for required content of breach notifications if breach notices will be sent to 500 or more individuals per Section (e)(8)(H). below.

(D) Annual Accounting

1. CDII Annual Breach Reporting
   The PO workforce shall submit an annual accounting of all PHI and PII breaches to CDII at the end of each calendar year or as requested. The information shall be submitted on the CDII Annual Breach Reporting form and shall include actions taken to investigate and mitigate each event.
2. HHS Annual Breach Reporting
   If fewer than 500 individuals are affected, the PO shall maintain a log documenting the breaches and assigned workforce shall submit breach information annually to HHS no later than 60 calendar days after the end of each calendar year on the Breach Reporting Log located on the HHS website at https://www.hhs.gov.

(E) The submission shall include all breaches discovered during the preceding calendar year.

(7) Breach Notification to Affected Individuals

(A) The PO workforce shall notify each individual who has had, or is reasonably believed to have had, health or personal information inappropriately accessed, acquired, used, or disclosed.

(B) PO workforce shall document and maintain all accounting of disclosure information, including the date of disclosure, name, and address of the entity who received the information, a brief description of the information disclosed, and a brief description of the cause of the disclosure.

(8) Content of Notification

The PO workforce shall provide notifications written in plain language and titled "Notice of Data Breach." It shall include all of the following, to the extent possible, using the prescribed headings:

(A) Using the title "What Happened," provide a brief description of what happened, including the date of the breach, the date the breach was discovered, and whether the notification was delayed due to a law enforcement investigation.

(B) Using the title "What Information Was Involved," the PO workforce shall describe the types of information involved in the breach (e.g., health information, full name, Social Security number, date of birth, and other identifiers).

(C) Using the title "What We Are Doing," the PO workforce shall briefly describe what the state entity is doing to investigate the breach, mitigate harm to the individuals, and protect against further breaches.

(D) Using the title "What You Can Do," the PO workforce shall advise individuals to take steps to protect themselves from potential harm resulting from the breach. The major credit reporting agencies' toll-free telephone numbers and addresses shall be included if the breach exposed PII such as Social Security number, driver's license number, California identification card number, or other personal identifiers.

1. **Credit Reporting Agency Information**
   a. Equifax Credit Information Services, LLC
      P.O. Box 740241, Atlanta, GA 30374
      1-888-548-7878
   b. Trans Union Consumer Relations
      P.O Box 2000, Chester, PA 19016-2000
      1-800-916-8800
   c. Experian National Consumer Assistance Center
      P.O. Box 4500, Allen, TX 75013
      1-800-493-1058

(E) Using the title "Other Important Information," the PO workforce shall provide the enclosure "Breach Help – Consumer Tips from the California Attorney General." This information is available in English and Spanish and can be downloaded from https://oag.ca.gov/privacy/other-privacy/breach-help-tips-for-consumers.

(F) Using the title "For More Information," the PO workforce shall provide the following statement "For information about your medical or personal privacy rights, you may visit the website of the California Department of Justice, Privacy Enforcement and Protection at https://oag.ca.gov/privacy."

(G) Using the title "Agency Contact," the PO workforce shall provide the name of the designated agency official or

agency unit handling inquiries along with a toll-free phone number and website.

(H) Before releasing the breach notification, the PO workforce shall:

1. Provide a draft of the breach notification to the CCHCS ISO for submission to the OIS using CAL-CSIRS for review and approval.
2. Electronically report the incident to the California Attorney General's office if the breach notification will be sent to more than 500 individuals.
3. Notify the CCHCS Director of Communications who shall provide a press release to the media when a breach affects more than 500 California residents.

(9) Methods of Notification

(A) Notification must be sent by first-class mail to the individuals' last known address.

1. An email is permitted if the individual agrees to electronic notice.
2. The PO workforce shall provide notification by telephone or other means as appropriate if it is determined that there is possible imminent misuse of any protected information.

(B) If the individual whose information has been breached is deceased, the next of kin or personal representative for the individual or patient shall be notified by first class mail.

(C) If the contact information is insufficient or out of date; preventing written notification to the individual, the PO workforce shall provide notice as follows:

1. The PO workforce notice via an alternate form of written notice, telephone, or other means may be provided when fewer than 10 individuals notified.
2. When more than 10 individuals are noticed, notice may be provided by a conspicuous posting for a period of 90 calendar days on the homepage of the CDCR or CCHCS website or by placing a conspicuous notice in a major print or broadcast media in the geographic area where the individuals affected by the breach likely reside.

(10) Timing of Notification

The PO workforce shall provide notifications in accordance with the following:

(A) When the situation or breach involves a clinic, health facility, home health agency, or hospice licensed by the CDPH, the PO workforce shall send a breach notification to the affected patient or patient's representative no later than 15 calendar days after the breach has been detected.

(B) A law enforcement agency may delay notification up to 60 calendar days with a written request or up to 30 calendar days with an oral request, if it is determined that notification will impede a criminal investigation.

(C) The PO workforce shall send a breach notification within 10 business days from the date a breach was reported, or reasonably believed to have occurred, to the extent possible. However, notice is required without unreasonable delay within and no later than 60 calendar days.

(D) Any decision to delay notification beyond 10 business days but less than 60 calendar days shall be made by the Privacy Officer in writing.

(11) Documentation Retention

The Privacy Officer shall retain this incident policy and procedure, all fact-finding, risk assessments, results, notifications, and reports for six years from the date of its creation, the date when it last was in effect, or whichever is later.

(12) Training Requirements and Contact Information.

(A) Privacy awareness training is required for all CCHCS workforce during New Employee Orientation and annually thereafter. All staff shall receive an annual reminder from the Learning Management System (LMS) to complete the Privacy Awareness Training. The PO workforce shall forward a copy of the training non-compliance report to the facility unit training coordinators for follow-up to ensure workforce completes the training. The training shall provide guidance on the use and protection of PHI, PII, and HRCI. All CCHCS workforce shall be required to review this policy and procedure in the LMS and acknowledge an understanding of this process.

(B) For questions or clarification, please contact CCHCSPrivacyOffice@cdcr.ca.gov or 1-877-974-4722.

Appendices

- Appendix 1: Workforce Privacy Incidents

References

- Code of Federal Regulations, Title 45, Subtitle A, Subchapter C, Part 164, Subpart D, Section 164.308(a)(1)(i)(D) and164.400 et seq.
- California Civil Code, Division 3, Part 4, Title 1.8, Chapter 1, Article 7, Section 1798.29
- California Civil Code, Division 1, Part 2.6, Section 56 et seq.
- California Health and Safety Code, Division 2, Chapter 2, Article 3, Section 1280.15
- California Code of Regulations, Title 22, Division 5, Chapter 13, Article 1, Section 79902
- California Department of Corrections and Rehabilitation, Department Operations Manual, Section 41010.3, Definitions – High Risk Confidential Information
- Health Care Department Operations Manual, Chapter 2, Article 2, Section 2.2.12, General Privacy Policies for Staff and Patient Information
- California Statewide Information Management Manual 5335-A, 5340-B-C
- 21st Century Cures Act, Public Law No 114-255 (12/13/2016)
- Coronavirus Aid, Relief, and Economic Security Act or the "CARES Act," Pub. L. No. 116-136 (2020)
- California Statewide Health Information Policy Manual (SHIPM) Chapter 3, Section 3.1.0, 3.1.4 III, A. 4, B 1.
- California State Administrative Manual, Sections 5305.7 (1), 5315, and 5335.2

Revision History
Effective: 09/2015
Revised: 11/01/2022

Appendix 1

Workforce Privacy Incidents

The following is a partial list of reportable incidents involving confidential or sensitive information

Workforce Decision-Based Privacy Incidents/Breaches (Most Common Types)

1. Emailing confidential patient or employee information to other areas, units, or offsite, such as labor organizations, Personnel, Performance Management Unit, etc.
2. Sending patient information to a global distribution list, and not everyone in that group has an authorized need to view the information.
3. Discussing patient or others confidential information in public areas.
4. Placing confidential documents in an open, unsecured shred box where others can view the information.
5. Not logging off the computer or a computer system that contains patient health or personal information before stepping away or when finished.
6. Intentionally sharing the confidential patient information of high notoriety patients or a patient's information during casual conversation with unauthorized individuals.
7. Accessing confidential electronic patient or personal information from an unsecured location.
8. Sharing confidential documents or a screenshot from the electronic medical record (Cerner) either hard copies or by email with unauthorized individuals.
9. Disclosing more than the minimum necessary information for treatment, payment, or health care operations.
10. Discarding confidential patient or personal information in the trash instead of shredding or proper disposal.
11. Posting information on Social Media.
12. Recording or photographing confidential information or inmates.
13. Using an electronic device containing confidential patient or personal information that is not password protected or encrypted.
14. Using unauthorized or personal electronic portable storage devices.
15. Discussing or using patients health or others personal information during staff meetings or when conducting group training.
16. Unauthorized access – Accessing confidential health information without an authorized reason, such as treatment, payment, or health care operations.
17. Sharing passwords or log in credentials.
18. Knowingly sending an unencrypted email that contains patient or employee confidential information.
19. Entering data related to another individual or third parties, such as family.
20. Disclosing a patient's health record that contains third party information.

Second Most Common Privacy Incidents/Breaches

1. Sharing patient information by 'selecting reply' all or using a distribution list containing multiple people who do not need to know the information.
2. Deliberately or inadvertently sending unencrypted email or attachments containing confidential Protected Health Information, Personally Identifiable Information, or other high-risk confidential information.
3. Using a personal home email account to send or receive confidential patient or personal information.
4. Selecting email recipients from the global email without verifying that you have chosen the correct individuals and subsequently addressing the email incorrectly including to someone in another agency.
5. Not considering whether there is a 'Need to Know.' Only those who are providing direct/related treatment, payment, or healthcare operations shall view a patients' information.
6. Using an outdated email distribution list that may contain the names of individuals who no longer work for the department or departmental workforce who no longer have a need to know.

Appendix 1

Other Common Types of Privacy Incidents/Breaches

1. Mistakenly discussing health information with the wrong patient.
2. Documenting or scanning health information to the wrong patient's electronic medical record.
3. Leaving information unattended or unsecured on a desk or in another work area.
4. Providing a patient with a packet of documents containing health or other sensitive information and mistakenly including another patient's health or sensitive information in the packet such as Release of Information, Appeals, or Grievances.
5. Disclosing lists containing patient information for those with COVID-19, receiving Substance Use Disorder Treatment (SUDT) or SUDT medications, etc., to those without a 'need to know'.