SOP Number	**1, January 2021**
SOP Title	**Care Plus Program SOCDIS Incident Management**

1. PURPOSE

To establish standard procedures to handle privacy and security incidents of protected health information (PHI), personal identifiable information (PII) and potential violations of state and federal privacy laws and County policies. This document describes the procedure for incident and breach management for the Care Plus Program related to privacy and security of the clients under care management in compliance with the applicable laws, policies and procedures.

2. BACKGROUND

Systems of Care Data Integration System (SOCDIS) is the database platform to facilitate the objectives of the Care Plus Program (CPP). CPP is the County's enhanced care coordination program which aims to improve the efficiency and effectiveness of Systems of Care. This minimizes delays in care coordination by maximizing employee skillset and resources and expedites identification, assessment and linkages to housing and supportive services. SOCDIS will facilitate access to data essential to care coordination, between departments.

3. SCOPE

The Office of Care Coordination (OCC) and County Privacy Officer in conjunction with OCIT, HCA IT and the Privacy Governance Committee shall implement guidelines, procedures and work flows in compliance with CPP Information Privacy and Security Policy to protect the privacy of sensitive personal information from unlawful or unauthorized access, use or disclosure.

All CPP Participating Agencies staff are responsible for reporting any known or suspected incidents of unacceptable access, use, or disclosure of sensitive personal or confidential information to the Office of Care Coordination in a timely manner.

4. TERMS OF USE

SOCDIS Participating Agencies must adhere to these terms of use and the following outlines a non-exhaustive list of what constitutes acceptable and unacceptable use:

Unacceptable use:

- The searching, viewing, amending of client information where the user has no involvement with the client or in the delivery of supportive services to that client.
- Creating records, forwarding or exchanging information, messages or email attachments that could breach the CPP Information Privacy and Security Policy.
- Improperly disclosing or misusing PII or PHI, or any other privileged or sensitive information.
- Breaching system integrity via compromising passwords e.g. by sharing it with others or writing it down, or by enabling access to an unlocked workstation.
- Intentionally hacking into or trying to access unauthorised areas of SOCDIS against the Role Based Access Control (RBAC) policy matrix.
- Any conduct which is criminal or otherwise unlawful or fraudulent.
- Storing, retaining or writing down PII or PHI outside of SOCDIS, unless critical in responding to an emergency / crisis situation.
- Unauthorised activities such as checking on family, neighbours, friends or associates for non-work related purposes.

Acceptable Use

- SOCDIS should be used for clients with whom authorization has been confirmed. Simpligov provides the platform for obtaining, amending and revocation of authorization.
- Declaration of any conflict of interest between a client and a system user must be made to OCC, prior to accessing the relevant client's file and prior to becoming part of that clients care team. Any actions deemed appropriate shall be taken at time of declaration.
- A participating agency must notify the OCC without due delay or at least within 24 hours if a system user account holder will cease to be employed or is suspended due to disciplinary action. System access will be removed or suspended as appropriate.

5. INCIDENT MANAGEMENT DEFINITIONS

Breach means the unauthorized access or acquisition of data that compromises the security,

confidentiality, or integrity of personally identifiable information (PII) and protected health information (PHI). Data may be in any format (electronic, hardcopy or verbal) and may consist of a single piece of data and/or an entire data system.

Discovery- a breach is treated as discovered on the first day that the breach is known by County staff or when by exercising reasonable diligence, the breach would have been known. *County Staff means employees, volunteers, trainees and other persons whose work is under direct control of the County.*

Individually Identifiable means that the medical information includes or contains any element of personal identifying information sufficient to allow identification of the individual, such as the patient's name, address, electronic mail address, telephone number, social security number, or other information that alone, or in combination with other publicly available information, reveals the individual's identity. *Medical Information means any individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care, health care service plan, pharmaceutical company, or contractor regarding a patient's medical history, mental or physical condition, or treatment (CA Civil Code § 56.05 (g)).*

Personally Identifiable Information (PII) is information that can be used alone, or in conjunction with other information to identify a specific individual. PII includes full name, Social Security Number, date of birth, driver's license number, or State issued identification number.

Protected Health Information (PHI) is individually identifiable health information held or transmitted in any form or medium by HIPAA covered entities and business associates. Unauthorized Access means the inappropriate review or viewing of patient medical information without a direct need for diagnosis, treatment, or other lawful use as permitted by the Confidentiality of Medical Information Act (Part 2.6 (commencing with Section 56) of Division 1 of the Civil Code) or by other statutes or regulations governing the lawful access, use, or disclosure of medical information. (CA Health & Safety Code § 130201 (e))

Unsecured Protected Health Information is protected health information that is not secured through the use of technology or methodology specified in Federal guidance documents to render PHI unusable, unreadable or indecipherable to unauthorized individuals. (HITECH § 13402 (h))

6. ROLES AND RESPONSIBILITIES

OC HCA IT

- Monitor system usage in coordination with OCC.
- Generate reports to validate user access in alignment with the policy matrix and RBAC (Role Based Access).
- HCA IT will act as a liaison between CPO, OCC and IBM to resolve any complex issues
- Detection and Reporting of unacceptable use.
- System monitoring and reporting to prevent and detect any unauthorized use or misuse of the system.

Office of Care Coordination

- Oversight of maintenance of the RBAC policy matrix.
- Point contact for initial notification of any potential unacceptable use, incident or breach.
- Completion, recording and updating of Confidentiality agreements and compliance trainings for all users prior to system access.
- Responsible for implementation of compliance training for the users and providers as appropriate.
- Repository for all CPP related documentation.
- Reviewing and assessing any conflict of interest disclosures.

OCIT – Enterprise Privacy & Cybersecurity

- Oversight and compliance with Care Plus Program Information Privacy and Security Policy and Privacy Governance Charter.
- Joint investigation of any unacceptable use, incident or breach.
- Adhere to the County guidelines of reporting incidents, investigations and corrective actions.
- Determine if a breach occurred and whether breach notification is required.
- Coordinate privacy and security incidents pertaining to the assigned agencies (i.e. SSA, OCCR, Probation).

Participating Agencies and Provider Portal Users

- Responsible for ensuring staff adhere to all policies and procedures, terms of use and for any disciplinary processes in event of breach of these policies.
- Notification to OCC of any conflict of interest declarations.
- Assigning a point person responsible for receiving and managing any RBAC policy matrix changes from their department and liaison with HCA IT / OCC to implement as recommended.
- New staff – orientation to system and completion of compliance trainings, confidentiality agreement and any other required program documentation.

7. PROCEDURE

When the Office of Care Coordination (OCC) or the County Privacy Office (CPO) is made aware of a privacy or security incident, OCC or CPO shall make contact with the program staff or program supervisor where the incident occurred and, if possible, immediately mitigate the risk of compromise to PHI. Mitigation may include, without limitation, retrieval of PHI, obtaining an attestation, securely deleting PHI from electronic files, and documenting the destruction of PHI erroneously sent.

After contact is made with program staff or program supervisor and any possible mitigation steps have been taken or instructed, have program staff or program supervisor complete and submit an Incident Intake Form online. The form can be accessed currently at: Radar Intake Form

When the Incident Intake Form has been received by OCC or CPO, it will be assigned within Radar® to the appropriate individual for handling.

Assigned Privacy or Security staff shall provide notification of the newly received incident to the Department privacy governance member assigned to the affected program and, when applicable, the following contacts based on Service Area:

Privacy governance members:

- Health Care Agency
- Social Services Agency
- OCCR
- OCPW
- OCSD
- Probation
- Departmental IT / OCIT

Compliance and Security will review the submitted Incident Intake form and determine if there are contractual reporting requirements based on the participating agencies.

Assigned Compliance or Security Staff will review and investigate the incident to determine if the incident poses a substantial risk that PHI was compromised.

8. REFERENCES

County of Orange breach reporting policy
https://www.ochealthinfo.com/occ/care_plus_program___internal/

9. CHANGE HISTORY

SOP no.	Effective Date	Significant Changes	Reviewed by
1	January 2021	New SOP	Melanie McQueen, Irfan Khan, Natalie Dempster, Linda Le