Docusign Envelope ID: 29BC9D0B-BE55-40A5-87E9-30F8A1ED8F96

Subject:	Compass OC Incident Management
Authority:	County Executive Office: Signature Signed by: Michelle Aguirre 1B08898A0E6A4EA...
Policy Owner:	CEO-Office of Care Coordination: Signature Signed by: Doug Becht 8A5EF37F35764E0...
Approval Date:	6/19/2024
Revision Date(s)	8/14/2025
Version No.:	2.0

A. Policy

Compass OC is the data integration platform used to facilitate the objectives of the Care Plus Program (CPP). The CPP is the County's enhanced care coordination program which aims to improve the efficiency and effectiveness of service delivery across the five components of the Systems of Care: Behavioral Health, Community Corrections, Healthcare, Housing, and Benefits and Support Services. The CPP aims to expedite the identification of client needs and subsequent linkages to services – resulting in greater collaboration, maximization of resources, and fewer delays in care coordination. Compass OC serves as a technology solution for CPP Participating Entities to access data essential for care coordination and provides a platform to create client care plans and track progress.

B. Purpose

To establish standardized procedures for managing privacy and security incidents involving Protected Health Information (PHI), Personally Identifiable Information (PII), and potential violations of state and federal privacy laws and County of Orange (County) policies. This document outlines the incident and breach management procedures specific to the CPP related to privacy and security of the clients under care management in compliance with the applicable laws, policies, and procedures.

C. Authority

The regulation, legislation, code or other requirement or entity that governs the policy. The Authority section is not applicable to all policies. Documentation associated with the Authority should be listed in the "References" section of the policy.

D. Scope

The Office of Care Coordination (OCC), in conjunction with Orange County Information Technology (OCIT) and the Privacy Governance Committee, shall implement guidelines, procedures, and workflows 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.

Docusign Envelope ID: 29BC9D0B-BE55-40A5-87E9-30F8A1ED8F96

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

TERMS OF USE

CPP Participating Entities must adhere to these terms of use. The following is a non-exhaustive list of what constitutes acceptable and unacceptable use of Compass OC:

Unacceptable Use

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

Acceptable Use

- Compass OC should be used for clients with whom authorization has been confirmed.
- 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 client's care team. Any actions deemed appropriate shall be taken at the time of declaration.
- A Participating Entity must notify the OCC without delay or within 24 hours if a Compass OC user account holder will cease to be employed or is suspended due to disciplinary action. Compass OC access will be removed or suspended as appropriate.

E. Responsibilities

OCIT

- OCIT served as the primary developer of Compass OC and will continue to work with the OCC to address any application issues that may arise.

Docusign Envelope ID: 29BC9D0B-BE55-40A5-87E9-30F8A1ED8F96

- Detecting 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.
- Generate reports to validate user access in alignment with the policy matrix and RBAC.
- Point contact for initial notification of any potential unacceptable use, incident or breach.
- Tracking of completion, recording and updating all CPP documents.
- Responsible for tracking and enforcement of CPP training for the users and Participating Entities, as appropriate.
- Reviewing and assessing any conflict-of-interest disclosures.

OCIT – Enterprise Privacy & Cybersecurity

- Oversight and compliance with CPP Information Privacy and Security Policy and Compass OC Incident Management Policy.
- Manage the annual CPP Training Campaigns.
- 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 Participating Entities (i.e., SSA, OCCR, Probation, HCA).

Participating Entity Users

- Responsible for ensuring staff adhere to all policies and procedures, terms of use and for any disciplinary processes in violation 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 OCIT / OCC to implement as recommended.
- New staff orientation to Compass OC and completion of compliance training, confidentiality agreement and any other required program documentation.

Docusign Envelope ID: 29BC9D0B-BE55-40A5-87E9-30F8A1ED8F96

F. Definitions

Term	Definition
Breach	The unauthorized access or acquisition of data that compromises the security, confidentiality, or integrity of Personally Identifiable Information (PII) or 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 that 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/or other persons whose work is under direct control of the County.
Individually Identifiable	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)	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)	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	Protected health information that is not secured using technology or methodology specified in Federal guidance documents to render PHI unusable, unreadable or indecipherable to unauthorized individuals. (HITECH § 13402 (h))

Docusign Envelope ID: 29BC9D0B-BE55-40A5-87E9-30F8A1ED8F96

G. Procedure

When the OCC or the County Privacy Officer is made aware of a privacy or security incident, the OCC and/or the County Privacy Officer shall contact the Participating Entity Privacy/Security staff, the program staff, and/or program supervisor where the incident occurred and, if possible, immediately mitigate the risk of compromise to PII/PHI. Mitigation may include, without limitation, retrieving PII/PHI, obtaining an attestation, securely deleting PII/PHI from electronic files, and documenting the destruction of PII/PHI inadvertently 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.

County Privacy Officer and/or OCC shall provide notification of the newly received incident to the Participating Entity Privacy Governance Committee member assigned to the affected program and, when applicable, the following contacts based on Service Area:

Privacy Governance Committee members:

- County Executive Office
- Office of Care Coordination
- County Counsel
- OC Community Resources
- OC Health Care Agency
- OC Information Technology
- OC Probation
- OC Public Defender
- OC Sheriff's Department
- OC Social Services Agency

County Privacy Officer and Participating Entity Privacy Governance Committee member will review the submitted Incident Intake form and determine if there are contractual reporting requirements based on the participating agencies.

County Privacy Officer will review and investigate the incident to determine if the incident poses a substantial risk that PII/PHI was compromised.

H. References

#	Title/URL
1	Care Plus Program | Orange County CEO's Office (ceo.ocgov.com)

Docusign Envelope ID: 29BC9D0B-BE55-40A5-87E9-30F8A1ED8F96

I. Change History

#	Version Updated Date	Description	Reviewed By
1	June 2024	New SOP	Zulima Lundy, Lisa Alford, Linda Le
2	August 2025	New Data Platform and CPP Steering Committee Membership	Julie Bechtol, Zulima Lundy, Linda Le