Policy:	HH.3020
Title:	**Reporting and Providing Notice of Security Incidents, Breaches of Unsecured PHI/PII or other Unauthorized Use or Disclosure of PHI/PII**
Department:	Office of Compliance
Section:	Privacy
CEO Approval:	*/s/ Michael Hunn 11/19/2024*
Effective Date:	07/01/2007
Revised Date:	11/07/2024
Applicable to:	☒ Medi-Cal ☒ OneCare ☒ PACE ☐ Administrative

I. PURPOSE

This policy describes CalOptima Health's policies and procedures for reporting Security Incidents, Breaches of Unsecured Protected Health Information/Personally Identifiable Information (PHI/PII) and/or other unauthorized access, Use, or Disclosure of PHI/PII to its regulators and providing notice to affected Members and media of Breaches of Unsecured PHI in accordance with contractual and regulatory requirements.

II. POLICY

A. CalOptima Health Employees shall immediately and no later than twenty-four (24) hours from time of discovery report any suspected or known Security Incidents, Breaches of Unsecured PHI/PII and/or other unauthorized access, Use, or Disclosure of PHI/PII to the CalOptima Health Privacy Officer, or Designee, in accordance with this Policy.

B. Business Associates shall notify CalOptima Health of discovery of any known or suspected Security Incidents, Breaches of Unsecured PHI/PII and/or other unauthorized access, Use, or Disclosure of PHI/PII immediately and no later than twenty-four (24) hours from time of discovery. Business Associates shall submit a written report to CalOptima Health of suspected, or known, Security Incidents, Breaches of Unsecured PHI/PII, and/or other unauthorized access, Use or Disclosure of PHI/PII, in accordance with this Policy.

C. CalOptima Health shall investigate such a Security Incident, Breach of Unsecured PHI/PII, and/or other unauthorized access, Use, or Disclosure of PHI/PII and provide a written report of the investigation to the Department of Health Care Services (DHCS) in accordance with this Policy.

D. CalOptima Health shall report Security Incidents, Breaches of Unsecured PHI/PII, or other unauthorized access, Use or Disclosure of PHI/PII to regulators, as required by its regulatory contracts and applicable state and federal laws.

E. CalOptima Health shall notify individual Members whose Unsecured PHI/PII has been or believed to have been accessed, acquired, Used, or Disclosed as a result of a Breach caused by CalOptima Health, which compromises the security or privacy of the PHI/PII.

F. CalOptima Health shall take appropriate actions to mitigate any harmful effect known to be caused by a Breach of Unsecured PHI/PII in accordance with CalOptima Health policy.

G. Except as otherwise provided in 45 CFR section 164.530(e)(1), CalOptima Health management, at its discretion, shall issue corrective action to Employees and persons in CalOptima Health's Workforce responsible for intentional or negligent actions that result in Security Incidents, Breaches of Unsecured PHI/PII, and/or other unauthorized access, Use, or Disclosure of PHI/PII in accordance with the HIPAA Violation Guidelines Matrix. CalOptima Health shall document any corrective actions that are applied.

H. Business Associates shall comply with CalOptima Health Business Associate Agreement reporting and notice requirements when a Security Incident, or Breach of Unsecured PHI/PII or other unauthorized access, Use, or Disclosure of PHI/PII involves DHCS and/or CalOptima Health PHI/PII.

III. PROCEDURE

A. Discovery

1. CalOptima Health Employees, Health Networks, with the exception of a Health Maintenance Organization (HMO) that satisfies the requirements of Section III.B.2. of this Policy, and Business Associates shall report any Security Incidents, Breaches of Unsecured PHI/PII, and/or other unauthorized access, Use, or Disclosure of PHI/PII immediately and no later than twenty-four (24) hours from time of discovery to the CalOptima Health Privacy Officer or Designee by telephone, fax, or email Privacy@caloptima.org.

    a. Examples of reportable Security Incidents or Breaches are:

        i. Lost or stolen unencrypted electronic devices that contain PHI or PII;

        ii. Posting PHI or PII on social media;

        iii. Emailing or saving EPHI to personal accounts and/or publicly accessible accounts;

        iv. Emailing EPHI that is not encrypted;

        v. Cybersecurity or hacking;

        vi. Downloading EPHI to a portable device in violation of CalOptima Health's policies (e.g., without expressed authority and required safeguards (encryption));

        vii. Faxes or emails that contain CalOptima Health PHI are misdirected to an unintended third party due to incorrect fax numbers or emails; and

        viii. Theft of paper records with CalOptima Health PHI from an Employee's vehicle.

B. The CalOptima Health Privacy Officer or Designee shall notify and report the discovery of any known or suspected Security Incidents, Breaches, Unsecured PHI/PII and/or other unauthorized access, Use, or Disclosure of PHI/PII to DHCS, in accordance with the following guidelines:

1. Notification to DHCS:

a. CalOptima Health shall notify DHCS immediately and no later than twenty-four (24) hours from the time of discovery of a suspected Breach, Security Incident, or unauthorized access, Use, or disclosure that involves SSA data. This notification will be provided through the DHCS Privacy Incident Reporting Portal . If CalOptima Health is unable to provide notification via the DHCS Privacy Incident Reporting Portal, then CalOptima Health shall provide notice by email or telephone to DHCS.

b. CalOptima Health shall notify DHCS within twenty-four (24) hours via the DHCS Privacy Incident Reporting Portal (by email or telephone if necessary) of the discovery of:

i. Unsecured PHI if the PHI is reasonably believed to have been accessed or acquired by an unauthorized person;

ii. Any suspected Security Incident which risks unauthorized access to PHI and/or other confidential information;

iii. Any Intrusion or unauthorized access, Use or disclosure of PHI in violation of CalOptima Health's Business Associate Agreement with DHCS; or

iv. Potential loss of confidential data affecting CalOptima Health's Business Associate Agreement with DHCS;

c. Notice shall be made via the DHCS Privacy Incident Reporting Portal and shall include all information known at the time the incident is reported.

d. The CalOptima Health Privacy Officer or Designee shall notify the DHCS Contract Manager, the DHCS Privacy Officer, and the DHCS Information Security Officer via the DHCS Privacy Incident Reporting Portal (by email or telephone, if necessary), as required and within twenty-four (24) hours.

2. Investigation and written report to DHCS:

a. Within ten (10) working days of the initial discovery, the CalOptima Health Privacy Officer or Designee shall submit a complete investigation report to the DHCS Contract Manager, DHCS Privacy Officer, and DHCS Information Security Officer by using the DHCS Privacy Incident Reporting Portal .

C. CalOptima Health shall notify Members whose Unsecured PHI/PII has been, or is believed to have been, accessed, acquired, Used, or Disclosed as a result of a Breach which compromises the security or privacy of the PHI. All notifications shall be provided without unreasonable delay and no later than sixty (60) calendar days from the date of discovery, which is the first day the Breach is known by a Covered Entity or would have been known by exercising reasonable diligence. CalOptima Health shall provide notification as specified below.

1. CalOptima Health shall write the notification in plain language and include, to the extent possible:

    a. A brief description of what occurred, including the date of the Breach and the date of the discovery of the Breach, if known;

    b. A description of the types of Unsecured PHI/PII that were involved in the Breach (e.g., full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information involved);

    c. Any steps Members should take to protect themselves from potential harm resulting from the Breach;

    d. A brief description of what the Covered Entity is doing to investigate the Breach, to mitigate harm to Members, and to protect against any further Breaches; and

    e. Contact procedures for Members to ask questions or learn additional information, which shall include a toll-free telephone number, an email address, website, or postal address.

2. CalOptima Health shall provide notification in the following form:

    a. CalOptima Health shall send written notification by first-class mail to the Member at the last known address. CalOptima Health may send written notification by electronic mail if the Member has agreed to receive notice by electronic mail and such agreement has not been withdrawn. CalOptima Health may provide notification in one (1) or more mailings as information is available.

        i. If the Member is deceased, CalOptima Health shall provide written notification by first- class mail to either the next of kin, or personal representative of the Member, if contact information is known.

        ii. If current contact information is unavailable for fewer than ten (10) Members, CalOptima Health may provide a substitute notice by an alternative form of written notice, telephone, or other means.

        iii. If current contact information is unavailable for ten (10) or more Members, CalOptima Health shall provide a substitute notice by a readily visible posting on the homepage of CalOptima Health's website for ninety (90) calendar days or by a readily visible notice in a major print or broadcast media in the geographic areas where the Members affected by the Breach likely reside. The notice shall include a toll-free telephone number that remains active for at least ninety (90) calendar days for Members to obtain information regarding the Breach.

    b. If CalOptima Health deems a Breach incident to require urgency because of a possible imminent misuse of Unsecured PHI/PII, CalOptima Health may provide Breach notification to Members by telephone or other means, in addition to written notice.

3. DHCS shall approve the time, manner and content of any such notifications and their review and approval must be obtained before the notifications are made.

D. The CalOptima Health Privacy Officer, or Designee, shall notify the Secretary of the U.S. Department of Health and Human Services (HHS) and Centers for Medicare & Medicaid Services (CMS) Account Manager immediately following the discovery of a Breach of Unsecured PHI /PII as follows:

1. For Breaches of Unsecured PHI/PII involving five hundred (500) or more Members, the CalOptima Health Privacy Officer, or Designee, shall provide notification to the Secretary of HHS.

2. For Breaches of Unsecured PHI/PII involving less than five hundred (500) Members, the CalOptima Health Privacy Officer, or Designee, shall submit a log of such Breaches for the preceding calendar year, no later than sixty (60) calendar days after the end of each calendar year.

E. For CMS reporting, CalOptima Health is required to follow the directions provided by HHS' Office for Civil Rights (OCR) related to the Health Information and Technology for Economic and Clinical Health (HITECH) breach notification regulations. Additional information, including a description of breach notification requirements, instructions for covered entities to submit breach notifications to the Secretary, and links to the online breach notification forms, can be found at: http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule

F. The CalOptima Health Privacy Officer, or Designee, shall notify the CMS Account Manager if there is the potential for significant Member harm (i.e., a high likelihood that the information was Used inappropriately) or situations that may have heightened public, or media, scrutiny (i.e., high number of Members affected, or particularly egregious Breaches). A "CMS Security and Privacy Incident Report" should be submitted for high-risk CalOptima Health breaches by email to CMS_IT_Service_desk@cms.hhs.gov. CalOptima Health shall report to the CMS Account Manager within two (2) business days of learning of a Breach that falls into these categories. The CalOptima Health Privacy department (Privacy) will include the Regulatory Affairs & Compliance (RAC) Medicare department (RAC Medicare) in this correspondence. In cases where CalOptima Health has notified OCR of the breach within this timeframe, CalOptima Health can send a copy of the breach report to the CMS Account Manager.

G. On a monthly basis, Privacy shall provide reported breaches to RAC Medicare via the CalOptima Health Compliance Log. If there were no breaches during a given month, a notification email shall be sent to RAC Medicare confirming that no breaches have occurred. RAC Medicare should provide updated reports to the CMS Account Manager as necessary.

H. The CalOptima Health Privacy Officer, or Designee shall notify the PACE Account Managers, and copy RAC Medicare, regarding security and privacy breaches involving PACE Participants. Breaches must be reported as soon as practical via email, using the "PACE Privacy Breach Notification Timeline and Summary" form.

I. For a Breach of Unsecured PHI/PII affecting more than five hundred (500) individuals, CalOptima Health shall notify prominent media outlets serving Orange County, in addition to providing individual written notices without unreasonable delay, but no later than sixty (60) calendar days from the date of discovery.

J. If a law enforcement official states to CalOptima Health that a notification, notice, or posting required under the Breach Notification Rule (45 CFR §§ 164.400-414) would impede a criminal investigation or cause damage to national security, CalOptima Health shall take the following action:

1. If the law enforcement official's statement is in writing and specifies the time for which a delay is required, CalOptima Health staff shall delay such notification, notice, or posting for the time period specified by the law enforcement official; or

2. If the law enforcement official's statement is made orally, CalOptima Health staff shall:

    a. Document the statement, including the identity of the official making the statement; and

    b. Delay the notification, notice, or posting temporarily and no longer than thirty (30) calendar days from the date of the oral statement, unless a written statement described in Section III.I. of this Policy is submitted during that time.

IV. ATTACHMENT(S)

A. HIPAA Violation Guidelines Matrix
B. CMS Security and Privacy Incident Report Form
C. PACE Privacy Breach Notification Timeline and Summary Form

V. REFERENCE(S)

A. CalOptima Health Business Associates Agreement
B. CalOptima Health Contract with the Centers for Medicare & Medicaid Services (CMS) for Medicare Advantage
C. CalOptima Health Contract with the Department of Health Care Services (DHCS) for Medi-Cal
D. CalOptima Health PACE Program Agreement
E. CalOptima Health Privacy Program
F. CalOptima Health Compliance Plan
G. CDA Program Memorandum PM 07-18(P): Protection of Information Assets
H. Department of Health Care Services (DHCS) All Plan Letter (APL) 06-001: HIPAA Requirements: Notice of Privacy Practices and Notification of Breaches
I. Department of Health Care Services (DHCS) All Plan Letter (APL) 06-005: Protected Health Information (PHI) and Notification of Breaches
J. Health Information and Technology for Economic and Clinical Health Act ("HITECH Act")
K. "Security and Privacy Reminders and Clarification of Reporting Procedures," Health Plan Management System (HPMS) Memorandum, Issued 12/16/2008
L. Title 45, Code of Federal Regulations §164.400 - 414 et seq.
M. Title 45, Code of Federal Regulations §164.502
N. Title 45, Code of Federal Regulations §164.514
O. Title 45, Code of Federal Regulations §164.530(e)(1)
P. Title 42 United State Code (U.S.C) §17932(h)
Q. "Update on Security and Privacy Breach Reporting Procedures," Health Plan Management System (HPMS) Memorandum, Issued 09/28/2010

VI. REGULATORY AGENCY APPROVAL(S)

Date	Regulatory Agency	Response
07/22/2013	Department of Health Care Services (DHCS)	Approved as Submitted
04/04/2022	Department of Health Care Services (DHCS)	Approved as Submitted
10/23/2023	Department of Health Care Services (DHCS)	File and Use

VII. BOARD ACTION(S)

Date	Meeting
12/01/2016	Regular Meeting of the CalOptima Board of Directors
12/07/2017	Regular Meeting of the CalOptima Board of Directors
12/06/2018	Regular Meeting of the CalOptima Board of Directors
12/05/2019	Regular Meeting of the CalOptima Board of Directors
12/03/2020	Regular Meeting of the CalOptima Board of Directors
12/20/2021	Special Meeting of the CalOptima Board of Directors
10/05/2023	Regular Meeting of the CalOptima Health Board of Directors
11/07/2024	Regular Meeting of the CalOptima Health Board of Directors

VIII. REVISION HISTORY

Action	Date	Policy	Policy Title	Program(s)
Effective	07/01/2007	HH.3020	Reporting a Breach of Data Security, Intrusion, or Unauthorized Use or Disclosure of Protected Health Information	Medi-Cal
Revised	01/01/2010	HH.3020	Reporting a Breach of Data Security, Intrusion, or Unauthorized Use or Disclosure of Protected Health Information	Medi-Cal
Revised	09/01/2011	HH.3020	Reporting a Breach of Data Security, Intrusion, or Unauthorized Use or Disclosure of Protected Health Information	Medi-Cal
Revised	01/01/2013	HH.3020	Reporting a Breach of Data Security, Intrusion, or Unauthorized Use or Disclosure of Protected Health Information	Medi-Cal
Revised	01/01/2014	HH.3020	Reporting a Breach of Data Security, Intrusion, or Unauthorized Use or Disclosure of Protected Health Information	Medi-Cal
Revised	11/01/2014	HH.3020	Reporting a Breach of Data Security, Intrusion, or Unauthorized Use or Disclosure of Protected Health Information	Medi-Cal
Revised	09/01/2015	HH.3020	Reporting a Breach of Data Security, Intrusion, or Unauthorized Use or Disclosure of Protected Health Information	Medi-Cal
Revised	12/01/2016	HH.3020	Reporting and Providing Notice of Security Incidents, Breaches of Unsecured PHI/PI or other Unauthorized Use or Disclosure of PHI/PI	Medi-Cal OneCare OneCare Connect PACE
Revised	12/07/2017	HH.3020	Reporting and Providing Notice of Security Incidents, Breaches of Unsecured PHI/PI or other Unauthorized Use or Disclosure of PHI/PI	Medi-Cal OneCare OneCare Connect PACE

Action	Date	Policy	Policy Title	Program(s)
Revised	12/06/2018	HH.3020	Reporting and Providing Notice of Security Incidents, Breaches of Unsecured PHI/PI or other Unauthorized Use or Disclosure of PHI/PI	Medi-Cal OneCare OneCare Connect PACE
Revised	12/05/2019	HH.3020	Reporting and Providing Notice of Security Incidents, Breaches of Unsecured PHI/PI or other Unauthorized Use or Disclosure of PHI/PI	Medi-Cal OneCare OneCare Connect PACE
Revised	12/03/2020	HH.3020	Reporting and Providing Notice of Security Incidents, Breaches of Unsecured PHI/PI or other Unauthorized Use or Disclosure of PHI/PI	Medi-Cal OneCare OneCare Connect PACE
Revised	12/20/2021	HH.3020	Reporting and Providing Notice of Security Incidents, Breaches of Unsecured PHI/PI or other Unauthorized Use or Disclosure of PHI/PI	Medi-Cal OneCare OneCare Connect PACE
Revised	12/31/2022	HH.3020	Reporting and Providing Notice of Security Incidents, Breaches of Unsecured PHI/PI or other Unauthorized Use or Disclosure of PHI/PI	Medi-Cal OneCare PACE
Revised	09/01/2023	HH.3020	Reporting and Providing Notice of Security Incidents, Breaches of Unsecured PHI/PI or other Unauthorized Use or Disclosure of PHI/PI	Medi-Cal OneCare PACE
Revised	11/07/2024	HH.3020	Reporting and Providing Notice of Security Incidents, Breaches of Unsecured PHI/PI or other Unauthorized Use or Disclosure of PHI/PII	Medi-Cal OneCare PACE

IX. GLOSSARY

Term	Definition
Breach	Has the meaning in 45, Code of Federal Regulations Section 164.402. Breach means the acquisition, access, Use, or Disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information. (1) Breach excludes: (i) Any unintentional acquisition, access, or Use of protected health information by a Workforce Member or person acting under the authority of a Covered Entity or a Business Associate, if such acquisition, access, or Use was made in good faith and within the scope of authority and does not result in further Use or Disclosure in a manner not permitted under subpart E of this part. (ii) Any inadvertent Disclosure by a person who is authorized to access protected health information at a Covered Entity or Business Associate to another person authorized to access protected health information at the same Covered Entity or Business Associate, or organized health care arrangement in which the Covered Entity participates, and the information received as a result of such Disclosure is not further Used or Disclosed in a manner not permitted under subpart E of this part. (iii) A Disclosure of protected health information where a Covered Entity or Business Associate has a good faith belief that an unauthorized person to whom the Disclosure was made would not reasonably have been able to retain such information.
Business Associate	Has the meaning given such term in Section 160.103 of Title 45, Code of Federal Regulations. A person or entity who: 1. On behalf of such Covered Entity or of an organized health care arrangement (as defined in this section) in which the Covered Entity participates, but other than in the capacity of a Member of the Workforce of such Covered Entity or arrangement, creates, receives, maintains, or transmits protected health information for a function or activity regulated by this subchapter, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities listed at 42 CFR 3.20, billing, benefit management, practice management, and repricing; or 2. Provides, other than in the capacity of a Member of the Workforce of such Covered Entity, legal, actuarial, accounting, consulting, data aggregation (as defined in §164.501 of this subchapter), management, administrative, accreditation, or financial services to or for such Covered Entity, or to or for an organized health care arrangement in which the Covered Entity participates, where the provision of the service involves the Disclosure of protected health information from such Covered Entity or arrangement, or from another Business Associate of such Covered Entity or arrangement, to the person.

Term	Definition
	A Covered Entity may be a Business Associate of another Covered Entity. Business Associate includes: 1. A Health Information Organization, E-prescribing Gateway, or other person that provides data transmission services with respect to protected health information to a Covered Entity and that requires access on a routine basis to such protected health information. 2. A person that offers a personal health record to one or more individuals on behalf of a Covered Entity. 3. A subcontractor that creates, receives, maintains, or transmits protected health information on behalf of the Business Associate.
Corrective Action Plan (CAP)	A plan delineating specific identifiable activities or undertakings that address and are designed to correct program deficiencies or problems identified by formal audits or monitoring activities by CalOptima Health, the Centers for Medicare & Medicaid Services (CMS), or designated representatives. FDRs and/or CalOptima Health departments may be required to complete CAPs to ensure compliance with statutory, regulatory, or contractual obligations and any other requirements identified by CalOptima Health and its regulators.
Covered Entity	A health plan, a health care clearinghouse, or a health care provider who transmits any health information in electronic form in connection with a transaction covered by Title 45, Code of Federal Regulations, Part 160.
Department of Health Care Services (DHCS)	The single State Department responsible for administration of the Medi-Cal program, California Children Services (CCS), Genetically Handicapped Persons Program (GHPP), and other health related programs as provided by statute and/or regulation.
Designee	A person selected or designated to carry out a duty or role. The assigned Designee is required to be in management or hold the appropriate qualifications or certifications related to the duty or role.
Disclosure	Has the meaning in 45, Code of Federal Regulations Section 160.103 including the following: the release, transfer, provision of access to, or divulging in any manner of information outside of the entity holding the information.
Employee	See below for definition of Workforce Member.
EPHI	Has the meaning in 45, Code of Federal Regulations Section 160.103. Individually identifiable health information transmitted by electronic media or maintained in electronic media.
Health Insurance Portability and Accountability Act (HIPAA)	The Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, was enacted on August 21, 1996. Sections 261 through 264 of HIPAA require the Secretary of the U.S. Department of Health and Human Services (HHS) to publicize standards for the electronic exchange, privacy and security of health information, and as subsequently amended.
Health Maintenance Organization (HMO)	A health care service plan, as defined in the Knox-Keene Health Care Service Plan Act of 1975, as amended, commencing with Section 1340 of the California Health and Safety Code.
Health Network	A Physician Hospital Consortium (PHC), physician group under a shared risk contract, or health care service plan, such as a Health Maintenance Organization (HMO) that contracts with CalOptima Health to provide Covered Services to Members assigned to that Health Network.

Term	Definition
Intrusion	The act of wrongfully (without authorization) entering upon, seizing, or taking possession of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by CalOptima Health or its Business Associates.
Member	A beneficiary enrolled in a CalOptima Health program.
Personally Identifiable Information (PII)	PII is ―any information about an individual maintained by an agency, including (1) any information that can be Used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, biometric records, race, ethnicity, language (REL), sexual orientation and gender identity (SOGI); and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.
Protected Health Information (PHI)	Has the meaning in 45 Code of Federal Regulations Section 160.103, including the following: individually identifiable health information transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium. This information identifies the individual or there is reasonable basis to believe the information can be Used to identify the individual. The information was created or received by CalOptima Health or Business Associates and relates to: 1. The past, present, or future physical or mental health or condition of a Member; 2. The provision of health care to a Member; or 3. Past, present, or future Payment for the provision of health care to a Member.
Security Incident	Has the meaning in 45 Code of Federal Regulations Section 164.304. The attempted or successful unauthorized access, Use, Disclosure, modification, or destruction of information or interference with system operations in an information system.
Unsecured Protected Health Information/Personal Information (PHI/PII)	Has the meaning in 45 Code of Federal Regulations Section 164.402. Protected Health Information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the Use of a technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of Public Law 111-5.
Use	Has the meaning in 45 Code of Federal Regulations Section 160.103, including the following: the sharing, employment, application, utilization, examination, or analysis of the PHI within an entity that maintains such information.
Workforce	Has the meaning given such term in Section 160.103 of Title 45, Code of Federal Regulations. Employees, volunteers, trainees, and other persons whose conduct in the performance of work for CalOptima Health is under the direct control of CalOptima Health, whether or not they are paid by CalOptima Health.

Term	Definition
Workforce Member	Has the meaning in 45, Code of Federal Regulations Section 160.103 including: Employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a Covered Entity or Business Associate, is under the direct control of such Covered Entity or Business Associate, whether or not they are paid by the Covered Entity or Business Associate.