Policy:	HH.3016
Title:	**Guidelines for Handling Protected Health Information Off-site**
Department:	Office of Compliance
Section:	Privacy
CEO Approval:	*/s/ Michael Hunn 11/19/2024*
Effective Date:	04/01/2003
Revised Date:	11/07/2024
Applicable to:	☒ Medi-Cal ☒ OneCare ☒ PACE ☐ Administrative

I. PURPOSE

This policy describes the process for handling Protected Health Information (PHI) created, accessed, or taken off-site from CalOptima Health offices.

II. POLICY

A. CalOptima Health employees shall exercise precautions according to the regulations and standards set by the Health Insurance Portability and Accountability Act (HIPAA) and CalOptima Health policies when handling PHI, or EPHI, created, accessed, or taken off-site from the main office.

III. PROCEDURE

A. General guidelines

1. Staff shall adhere to Minimum Necessary requirements when viewing, documenting, and/or recording information during any work activities that require the Use of Medical Records in facilities.

2. Staff shall not access, use, or disclose any Member PHI via CalOptima Health system without a business need.

3. Staff shall collect all data relative to a Member, whether by interview, observation, or review of documents, in a setting that provides reasonable privacy and protects the information from unauthorized Disclosure.

4. Staff shall protect all physical documents that contain Member PHI from the view, or access, by an unauthorized person during transport from and to the office through Use of:

   a. Binders; and/or

   b. Folders, or other protective cover; and/or

   c. Appropriate vehicle safeguards (e.g., locked in trunk of the vehicle); or

   d. Personal possession of Member PHI such that it is in sight at all times.

5. Staff shall not leave any paper documents containing PHI, or other data collection forms including, without limitation, audit or other data collection forms unattended in areas accessible by an unauthorized person.

6. Staff shall not store confidential, personal, or sensitive information unattended in vehicles at any time.

7. Staff shall not store confidential, personal, or sensitive information unattended in baggage, at any time, during travel.

8. Staff shall not save or store data files in an electronic format that contain PHI on public, or private, computers, unencrypted personal removable storage devices, personal cloud storage, and/or personal email accounts.

9. Staff shall not Use mobile devices of any kind to take and save photos of information and/or images containing PHI.

10. Staff shall maintain physical control of CalOptima Health laptops, cell phones, tablets, USB drives, and all other mobile devices at all times.

11. Staff shall only Use CalOptima Health-issued encrypted storage devices to store files containing PHI, in accordance with CalOptima Health Policy GA.5005a: Use of Technology Resources.

12. Staff shall shred PHI documents, or files, prior to disposal. If necessary, staff shall return documents, or files, to the main office for disposal.

B. Use of Personal Computer (PC) from remote locations

1. If applicable, employees granted access to CalOptima Health's networks are required to adhere to the following procedures:

a. Maintain the Confidentiality of his or her user sign-on identification code and password;

b. Keep the PC secure at all times and do not leave it unattended during travel to, or working off-site at, public places (e.g., hospitals, Long Term Care (LTC) facilities, conferences, etc.);

c. Log off the CalOptima Health network, or lock computer, when the PC will be left inactive, or unattended; and

d. Ensure that passwords, or operating instructions for accessing the CalOptima Health systems, are not stored with the computer.

C. CalOptima Health employees, Business Associates, and First Tier, Downstream, and Related Entities (FDRs) shall report any Security Incidents, Breaches of Unsecured PHI/PI and/or other unauthorized access, Use, or Disclosure, of PHI/PI immediately after discovery during a workweek to the CalOptima Health Privacy Officer, in accordance with CalOptima Health Policy HH.3020: Reporting and Providing Notice of Security Incidents, Breaches of Unsecured PHI/PI or other unauthorized Use or Disclosure of PHI/PI.

IV. ATTACHMENT(S)

Not Applicable

V. REFERENCE(S)

A. CalOptima Health Contract with the Centers for Medicare & Medicaid Services (CMS) for Medicare Advantage
B. CalOptima Health Contract with the Department of Health Care Services (DHCS) for Medi-Cal
C. CalOptima Health PACE Program Agreement
D. CalOptima Health Compliance Plan
E. CalOptima Health Policy GA.5005a: Use of Technology Resources
F. CalOptima Health Policy HH.3020: Reporting and Providing Notice of Security Incidents, Breaches of Unsecured PHI/PI or other Unauthorized Use or Disclosure of PHI/PI
G. CalOptima Health Policy IS.1102: Electronic Media, Electronic Storage Device and Hardware Controls
H. CalOptima Health Policy IS.1201: EPHI Technical Safeguards - Access Controls
I. Health Administrative Manual
J. Title 45, Code of Federal Regulations (C.F.R.), §164.103
K. Title 45, Code of Federal Regulations (C.F.R.), §164.502(b)
L. Title 45, Code of Federal Regulations (C.F.R.), §164.530(c)(1)

VI. REGULATORY AGENCY APPROVAL(S)

Date	Regulatory Agency	Response
09/21/2009	Department of Health Care Services (DHCS)	Approved as Submitted
07/16/2010	Department of Health Care Services (DHCS)	Approved as Submitted

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
11/07/2024	Regular Meeting of the CalOptima Health Board of Directors

VIII. REVISION HISTORY

Action	Date	Policy	Policy Title	Program
Effective	04/01/2003	HH.3016	Guidelines for Handling Protected Health Information Offsite	Medi-Cal
Revised	04/01/2007	HH.3016	Guidelines for Handling Protected Health Information Offsite	Medi-Cal
Revised	01/01/2009	HH.3016	Guidelines for Handling Protected Health Information Offsite	Medi-Cal
Revised	06/01/2010	HH.3016	Guidelines for Handling Protected Health Information Offsite	Medi-Cal
Revised	04/01/2013	HH.3016	Guidelines for Handling Protected Health Information Offsite	Medi-Cal
Revised	09/01/2015	HH.3016	Guidelines for Handling Protected Health Information Offsite	Medi-Cal

Action	Date	Policy	Policy Title	Program
Revised	12/01/2016	HH.3016	Guidelines for Handling Protected Health Information Offsite	Medi-Cal OneCare OneCare Connect PACE
Revised	12/07/2017	HH.3016	Guidelines for Handling Protected Health Information Offsite	Medi-Cal OneCare OneCare Connect PACE
Revised	12/06/2018	HH.3016	Guidelines for Handling Protected Health Information Offsite	Medi-Cal OneCare OneCare Connect PACE
Revised	12/05/2019	HH.3016	Guidelines for Handling Protected Health Information Offsite	Medi-Cal OneCare OneCare Connect PACE
Revised	12/03/2020	HH.3016	Guidelines for Handling Protected Health Information Offsite	Medi-Cal OneCare OneCare Connect PACE
Revised	12/20/2021	HH.3016	Guidelines for Handling Protected Health Information Offsite	Medi-Cal OneCare OneCare Connect PACE
Revised	12/31/2022	HH.3016	Guidelines for Handling Protected Health Information Offsite	Medi-Cal OneCare PACE
Revised	09/01/2023	HH.3016	Guidelines for Handling Protected Health Information Offsite	Medi-Cal OneCare PACE
Revised	11/07/2024	HH.3016	Guidelines for Handling Protected Health Information Offsite	Medi-Cal OneCare PACE

IX. GLOSSARY

Term	Definition
Access Controls	Controls that identify and authenticate a User to allow access to confidential information and Protected Health Information (PHI) based on a business need to know. Access Controls protect the computer systems from unauthorized access as well as determine the type of access a User is entitled to have.
Breach	Has the meaning in 45, Code of Federal Regulations Section 164.402. 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. Breach excludes: 1. 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. 2. 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. 3. 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
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.
Downstream Entity	Any party that enters into an acceptable written arrangement below the level of the arrangement between a Medicare Advantage (MA) organization (and contract applicant) and a First Tier Entity. These written arrangements continue down to the level of the ultimate provider of health and/or administrative services.
Electronic Protected Health Information (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.
Facility	Off-site, CalOptima Health-affiliated locations; any site outside of the 505 City Parkway West building.
First Tier, Downstream, and Related Entities (FDR)	Means First Tier, Downstream or Related Entity, as separately defined herein.
First Tier Entity	Any party that enters into a written arrangement, acceptable to CMS, with an MAO or Part D plan sponsor or applicant to provide administrative services or health care services to a Medicare eligible individual under the MA program or Part D program.
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.
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.

Term	Definition
Long Term Care (LTC)	Medi-Cal: Care provided in a skilled nursing facility and sub-acute care services that lasts longer than 60 days. OneCare: A variety of services that help Members with health or personal needs and activities of daily living over a period of time. Long Term Care (LTC) may be provided at home, in the community or in various types of facilities, including nursing homes and assisted living facilities.
Medical Record	Medi-Cal: Any single, complete record kept or required to be kept by any Provider that documents all the medical services received by the Member, including, but not limited to, inpatient, outpatient, and emergency care, referral requests, authorizations, or other documentation as indicated by CalOptima Health policy. OneCare: A Medical Record, health record, or medical chart in general is a systematic documentation of a single individual's medical history and care over time. The term 'Medical Record' is Used both for the physical folder for each individual patient and for the body of information which comprises the total of each patient's health history. Medical Records are intensely personal documents and there are many ethical and legal issues surrounding them such as the degree of third-party access and appropriate storage and disposal.
Member	A beneficiary enrolled in a CalOptima Health program.
Minimum Necessary	The principle that covered entity must make reasonable efforts to Use, disclose, and request only the minimum amount of protected health information needed to accomplish the intended purpose of the Use, Disclosure, or request for Treatment, Payment or Health Care Operations.
Prior Authorization	Medi-Cal: A formal process requiring a health care Provider to obtain advance approval of Medically Necessary Covered Services, including the amount, duration and scope of services, except in the case of an emergency. OneCare: A process through which a physician or other health care provider is required to obtain advance approval, from CalOptima Health and/or a delegated entity, that payment will be made for a service or item furnished to a Member. PACE: A formal process requiring a health care provider to obtain advance approval to provide specific services or procedures, or the process by which an IDT approves a member to receive a specific service or procedure.
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, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

Term	Definition
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. Individually identifiable health 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.
Related Entity	Any entity that is related to CalOptima Health by common ownership or control and that: performs some of CalOptima Health's management functions under contract or delegation; furnishes services to Members under an oral or written agreement; or leases real property or sells materials to CalOptima Health at a cost of more than two thousand five hundred dollars ($2,500) during a contract period.
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 PHI/PI	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.