Policy:	IS.1600
Title:	**Provider Access to In-House Provider Portal**
Department:	Information Services
Section:	Not Applicable
CEO Approval:	*/s/ Richard Sanchez 08/05/2021*
Effective Date:	08/05/2021
Revised Date:	Not Applicable
Applicable to:	☐ Medi-Cal ☐ OneCare ☐ OneCare Connect ☐ PACE ☒ Administrative

I. PURPOSE

This policy defines the standards and procedures pursuant to which Provider Office Users shall be permitted to use CalOptima's In-House Provider Portal ("Provider Portal").

II. POLICY

A. The Provider Portal is an information system developed by CalOptima which grants authorized Provider Office Users access to Protected Health Information ("PHI") to carry out Payment and Health Care Operations for CalOptima's eligible Members.

B. The Provider Portal is available to Provider Office Users with a registered user account.

C. Role-based user assignment shall be implemented to comply with the Principle of Least Privilege within the Provider Portal, and Users shall be granted only the Minimum Necessary Access to the data that is required for the User to perform the User's specific job-related duties, in accordance with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").

D. Most of the information contained within the Provider Portal is confidential and protected by HIPAA. Provider Office Users are authorized to use such information for the sole purpose of carrying out Payment and Health Care Operations. Users are prohibited from downloading, printing, copying, taking a screen shot of, or forwarding Provider Portal information or documents for purposes other than Payment and Health Care Operations.

E. Controls to Prevent Unauthorized Access to PHI

1. A Provider Office shall take reasonable and appropriate measures to control unauthorized access to PHI in oral and electronic forms.

2. To the extent a Provider Office or its Users print and/or copy Provider Portal information or documents for purposes of Payment or Health Care Operations, a Provider Office shall take reasonable and appropriate measures to control unauthorized access to PHI in paper form.

F. All records referring to or containing Restricted Information shall be suppressed from view within the Provider Portal.

G. CalOptima implements Administrative and Technical Safeguards in compliance with HIPAA, and in accordance with CalOptima Policies, including, but not limited to, CalOptima Policies IS.1601: In-House Provider Portal Administration and Support (Internal) and HH.3002Δ: Minimum Necessary Uses and Disclosure of Protected Health Information and Document Controls.

H. CalOptima monitors and reviews all access to and use of the Provider Portal, in accordance with CalOptima Policy IS.1303Δ: Audit, Review, Testing, and Change Management.

I. CalOptima shall establish a CalOptima Provider Portal User Agreement and Terms and Conditions of Use (Attachment A), review it annually and update its terms as necessary.

J. CalOptima shall ensure that all Provider Office User(s) complete and attest to the Provider Portal User Training on an annual basis.

K. CalOptima may impose Sanctions on a Provider Office and/or Provider Office User(s) found in violation of this policy, the CalOptima Provider Portal User Agreement and Terms and Conditions of Use, or the Provider Portal Access Agreement.

    1. The extent of the Sanction shall be commensurate with the severity of the deficiency identified as it relates to the risk posed to the CalOptima Member(s) and shall be designed to correct the underlying issue to prevent future recurrence. Sanctions include, but are not limited to Corrective Action Plans, re-education and/or termination of access for Provider Office Users.

L. Any person with knowledge of a violation, or potential violation, of this Policy shall report such information to the Privacy Officer directly, or through the CalOptima Compliance and Ethics Hotline at 1-877-837-4417 or email: privacy@caloptima.org in accordance with CalOptima Policy HH.3020Δ: Reporting and Providing Notice of Security Incidents, Breaches of Unsecured PHI/PI or other Unauthorized Use or Disclosure of PHI/PI.

III. PROCEDURE

A. Provider Office User Account Registration

    1. To request access to CalOptima's Provider Portal, the following must occur:

        a. The Provider Office will complete and sign the Provider Portal Access Agreement (Attachment C) for Provider Office Entity and return it to CalOptima prior to access being permitted by CalOptima.

        b. Each Provider Office shall designate a Local Office Administrator who is responsible for approving Provider Office User account requests and for granting permissions to access the Provider Portal as needed to carry out their specific job-related duties.

        c. Provider Office Users must:

            i. Supply the following information using the Provider Portal registration form:

                a) First name;

                b) Last name;

                c) Street address;

d) City;

e) Zip code;

f) Phone number; and

g) Email address.

h) Job position and/or title

ii. Specify the Provider Office to which they are affiliated.

iii. Verify that they have access to the email address using a one-time passcode that is sent to the email address during account registration.

iv. Agree to the requirements set forth on the CalOptima Provider Portal User Agreement and Terms and Conditions of Use.

v. Complete and attest to the Provider Portal User Training.

B. Provider Office User Account Setup and Validation

1. Upon completion of account registration, the Provider Portal system will route the access request to the Local Office Administrator for review and approval.

2. In the event there is no designated Local Office Administrator for the specified Provider Office, the system will route the access request to the Enterprise Administrator queue.

3. Access requests must be approved or denied by the Local Office Administrator or an Enterprise Administrator.

a. For access requests that are approved by the Local Office Administrator, the system will store the approval date along with the name of the Local Office Administrator that approved the request.

b. For Provider Offices with no existing Local Office Administrators, the access request will be routed to the Enterprise Administrators within CalOptima. The Enterprise Administrator will reach out to the Provider Office Manager to assist with the Provider Office User request. In addition, the Enterprise Administrator will coordinate with the Provider Office Manager to establish a Local Office Administrator responsible for validating and approving access requests.

4. Upon approval of the access request, the registrant will receive an email that their account has been approved.

5. Upon denial of the access request, the registrant will receive an email that their request has been denied.

6. The Local Office Administrator shall review a User's job description to determine the appropriate level of access needed and grant the approved Provider Office User within their Provider Office with access to one or more of the following user roles, as applicable and necessary for the User to perform the User's specific job-related duties:

a. Eligibility Viewer: Grants Users access to view Member eligibility.

b. Claims Viewer: Grants Users access to view claims that belong to the Provider Office.

c. View Referrals: Grants Users access to view referrals that belong to the Provider Office.

d. Submit Referrals: Grants Users the ability to submit referrals to CalOptima.

7. The Local Office Administrator shall limit access to a Member's PHI to only those Provider Officer Users who need to Use the data to carry out their specific job-related duties related to Payment or Health Care Operations.

8. The Local Office Administrator may grant access to Provider Office Users on a specific "need-to-know" basis and shall restrict access to the minimum amount of PHI needed to complete the work activity.

9. The Local Office Administrator shall attest that the access designated to the Provider Office User is necessary to perform their job duties and complies with the Principle of Least Privilege and Minimum Necessary standard.

C. User Identification

1. Provider Office Users are identified by their email address.

2. Once the account has been created, the email address may not be changed.

3. The email address must be unique.

4. The email address must adhere to the following format requirements:

a. Must contain an at symbol (i.e., @); and

b. Must include a valid domain and extension (e.g., "User@registereddomain.com").

D. Passwords

1. Once a Provider Office User account is approved, the Provider Office User is required to establish an account password.

2. The account password may be changed by the Provider Office User at any time.

3. The password must meet the conditions specified below:

a. The password must contain at least 7 characters

b. The password must contain at least three of the following character types:

i. One lower case letter

ii. One upper case letter

iii. One number

iv. A special character (!,@,#,$,%,*, etc.)

4. The account password must not be the same as the email address.

5. The account password must be reset every sixty (60) calendar days.

E. Login

1. Provider Office Users must enter a valid email address and password in order to access the Provider Portal.

2. The User's login session will be closed after 15 minutes of inactivity.

3. Permission to access the Provider Portal is locked after five (5) failed login attempts. Specifically, where the input value for password does not match the specified login identifier.

4. To regain access to a locked Provider Portal account, Provider Office Users must:

   a. Contact an Enterprise Administrator; or

   b. Reset their password

F. Two-Factor Authentication

1. As an added layer of security, Provider Office Users shall complete two-factor Authentication:

   a. When logging in to the Provider Portal for the first time;

   b. When logging in to the Provider Portal using an unknown device;

   c. When the Provider Office User attempts to view or update their User accounts, using the following self-service tools:

      i. Forgot password;

      ii. Reset password; or

      iii. Update User profile

2. Provider Office Users shall complete two-factor Authentication as follows:

   a. By entering a security passcode delivered to the registered User's email address or mobile phone; or

   b. By answering security questions established during account registration.

3. Security passcodes delivered via email address or mobile phone are six (6) numeric characters in length and expire within fifteen (15) minutes.

G. User Administration

1. Provider Office Users may update their User information, except email address, through the Provider Portal's, "Update User Profile" interface.

H. Local Office Administrator Verification of Provider Office Users

1. Every forty-five (45) calendar days, commencing upon the date the Provider Office obtains access to the Provider Portal, each Local Office Administrator will be prompted to verify the Users for their corresponding Provider Office, including, each and every User's employment status, role, and security setting.

2. Any Local Office Administrator who has not completed the User verification within fifteen (15) calendar days of receiving the above-mentioned prompt will be restricted from navigating throughout the application until the verification is complete.

3. CalOptima shall systematically suspend access to the Provider Portal for every account associated with the Provider Office for failure to complete User verification within sixteen (16) calendar days of receiving the above-mentioned prompt. Each User will be notified upon login attempt that their account has been suspended.

4. Local Office Administrators may contact CalOptima's Provider Relations Department to complete the User verification process and request reinstitution of access to the Provider Portal.

5. Once the User verification process is complete, CalOptima's Provider Relations Department will contact e-Business to reinstate Provider Portal access to the Provider Office and its verified Users.

I. Restricted Information

1. CalOptima shall suppress all records referring to or containing Restricted Information from view within the Provider Portal, and Users shall not have access to such information through the Provider Portal. This includes:

    a. Birth Control
    b. Pregnancy
    c. Abortion
    d. STIs, Contagious and Reportable Diseases
    e. HIV/AIDS Treatment and Testing
    f. Sexual Assault Care
    g. Alcohol/Drug Counseling
    h. Outpatient Mental Health Treatment

2. CalOptima's Information Services Department shall maintain a list of diagnosis codes, procedure codes, and medications which will be restricted from view within the Provider Portal for all Users.

3. On a monthly basis, CalOptima will review the list of diagnosis codes, procedure codes, and medications to capture any changes, including additions or deletions, to such codes and medications.

J. Annual User Training

1. On an annual basis each Provider Office User will be prompted to complete and attest to the Provider Portal User Training.

2. Provider Office User(s) who have not completed and attested to the Provider Portal User Training by the required date specified by CalOptima will be restricted from accessing the Provider Portal until the training and attestation is complete.

3. Once the Provider Portal User Training and attestation are complete, the User will regain access to the Provider Portal.

K. Reporting, Responding to, and Investigating Breaches, Security Incidents, Violations, or Noncompliance with the CalOptima Provider Portal User Agreement and Terms and Conditions of Use

1. Local Office Administrators, Provider Offices, and Users are responsible for reporting any suspected, potential, or actual Security Incidents, Breaches, Violations, or noncompliance with the CalOptima Provider Portal User Agreement and Terms and Conditions of Use to CalOptima's Privacy Officer via email (Privacy@CalOptima.org) or through the CalOptima Compliance and Ethics Hotline at 1-877-837-4417, immediately, but no later than twenty-four (24) hours after discovery. Any suspected, potential, or actual Security Incident, Breach, Violation, or noncompliance with the CalOptima Provider Portal User Agreement and Terms and Conditions of Use shall be treated as discovered by the Local Office Administrator, Provider Office, or User as of the first day on which it is known, or by exercising reasonable diligence would have been known, to any person who is a part of the Workforce (excepting the person committing the Security Incident, Breach, Violation, or noncompliance with the CalOptima Provider Portal User Agreement and Terms and Conditions of Use).

2. Upon discovery of a Security Incident, Breach, Violation, or noncompliance with the CalOptima Provider Portal User Agreement and Terms and Conditions of Use, the Provider Office and its Local Office Administrator shall:

a. Take prompt action to mitigate, to the extent practicable, any risks or damages involved with the Security Incident, Breach, Violation, or noncompliance with the CalOptima Provider Portal User Agreement and Terms and Conditions of Use. Notwithstanding the foregoing, all corrective actions are subject to the approval of CalOptima and CalOptima's regulator(s).

b. Take any action pertaining to such Security Incident, Breach, Violation, or noncompliance with the CalOptima Provider Portal User Agreement and Terms and Conditions of Use required by applicable Federal and State laws and regulations.

c. Take any corrective actions required by CalOptima and CalOptima's regulator(s).

d. Immediately investigate such Security Incident, Breach, Violation, or noncompliance with CalOptima Provider Portal User Agreement and Terms and Conditions of Use, and within forty-eight (48) hours of the discovery, notify CalOptima of the matters described below.

i. The date of the Security Incident, Breach, Violation, or noncompliance with CalOptima Provider Portal User Agreement and Terms and Conditions of Use and the date it was discovered;

ii. A description of the probable causes of the Security Incident, Breach, Violation, or noncompliance with the CalOptima Provider Portal User Agreement and Terms and Conditions of Use;

iii. A description of the unauthorized persons known or reasonably believed to have improperly Used or Disclosed PHI or confidential data;

iv. The nature of the PHI or confidential data elements involved and the extent of the PHI or confidential data involved in the Security Incident, Breach, Violation, or noncompliance with the CalOptima Provider Portal User Agreement and Terms and

Conditions of Use and whether the PHI or confidential data that is the subject of the Security Incident, Breach, Violation, or noncompliance with the CalOptima Provider Portal User Agreement and Terms and Conditions of Use included Unsecured Protected Health Information;

v. A description of where the PHI or confidential data is believed to have been improperly transmitted, sent, or utilized;

vi. The identification of each individual whose Unsecured PHI has been, or is reasonably believed by the Provider Office and Local Office Administrator to have been accessed, acquired, used or disclosed during the Security Incident, Breach, Violation, or noncompliance with the CalOptima Provider Portal User Agreement and Terms and Conditions of Use;

vii. Any other available information that the Provider Office is required to include in notification to the individual under 45 C.F.R. § 164.404(c);

e. Provider Office shall make itself and any of its subcontractors, employees or agents available to CalOptima at no cost to CalOptima to testify as witnesses or otherwise in the event of litigation or administrative proceedings being commenced against CalOptima, its directors, officers or employees based upon claimed violation of HIPAA, the HITECH Act and/or implementing regulations and/or State privacy laws, which involve actions or inactions by the Provider Office or its Workforce related to the Provider Portal, except where Provider Office or its subcontractor, employee or agent is named as an adverse party.

3. In the event CalOptima staff is made aware of an actual, suspected, or potential Security Incident, Breach, Violation, or noncompliance with the CalOptima Provider Portal User Agreement and Terms and Conditions of Use, CalOptima staff shall comply with the procedures and requirements in CalOptima Policy HH.3020Δ: Reporting and Providing Notice of Security Incidents, Breaches of Unsecured PHI/PI or other Unauthorized Use or Disclosure of PHI/PI, including, but not limited to, immediately notifying the CalOptima Privacy Officer or Designee by telephone, fax, or email Privacy@caloptima.org.

4. If CalOptima's Privacy Office and/or Information Services Security is made aware of an actual, potential, or suspected Security Incident, Breach, Violation, or noncompliance with the CalOptima Provider Portal User Agreement and Terms and Conditions of Use, they will contact the Enterprise Administrator to suspend the User(s) account(s) pending further investigation.

5. Enterprise Administrators must suspend a User's account immediately upon receiving a report of an actual, potential, or suspected Security Incident, Breach, Violation, or noncompliance with the CalOptima Provider Portal User Agreement and Terms and Conditions of Use.

6. CalOptima's Privacy Office and/or Information Services Security department will contact the CalOptima's Provider Relations Department to assist with the investigation, including Provider outreach and education, if necessary.

a. Provider Offices, Local Office Administrators and Users must cooperate and assist CalOptima's Privacy Officer and/or Security Officer with the investigation of actual, suspected, or potential Security Incidents, Breaches, Violation, or noncompliance with the CalOptima Provider Portal User Agreement and Terms and Conditions of Use occurring in their office or committed by their current or former employees.

b. During an investigation, the Local Office Administrator, Provider Office, and Users must respond to and fully comply with all requests for information or documents within the time specified by the CalOptima Privacy Officer and/or Security Officer in order to ensure CalOptima meets regulatory requirements for reporting Breaches, Security Incidents, Violations, or noncompliance with the CalOptima Provider Portal User Agreement and Terms and Conditions of Use.

7. Upon completion of the investigation, CalOptima's Privacy Office and/or Information Services Security, in conjunction with Provider Relations and e-Business, will make a recommendation on corrective actions. Examples of corrective actions may include, but are not limited to, Provider Office re-education, Provider User training, Corrective Action Plan(s), and termination of User account(s).

8. CalOptima's Privacy Office and/or Information Services Security department will contact an Enterprise Administrator to reinstate accounts at the conclusion of such investigations, as applicable.

9. CalOptima may revoke access to all Provider Office Users associated with a Provider Office and its Workforce if the non-compliance action deems necessary.

L. User Activity Logs

1. CalOptima shall log User account activity, including Authentication successes and failures, in accordance with CalOptima Policy IS.1303Δ: Audit, Review, Testing, and Change Management.

2. Each page visited by a Provider Office User will be recorded in a secure audit log as new row record containing the date and time, and the email address of the User that viewed the record.

3. Changes to the Provider Office User record will be reflected in a secure audit log as a new row record containing the date and time of change, and the email address of the User that made the change.

4. Access to Provider Office User activity logs shall be limited to authorized managers and Enterprise Administrators.

5. User activity logs shall be retained according to CalOptima Policy HH.2022Δ: Record Retention and Access.

M. Terminated User Accounts

1. A Provider Office User whose account has not been used for over sixty (60) calendar days shall not be able to log into the Provider Portal.

2. A Provider Office User whose account has been disabled by either a Local Office Administrator or an Enterprise Administrator shall not be able to login to the Provider Portal.

3. The Local Office Administrator is responsible for immediately terminating or limiting, as applicable, User access for staff who are no longer employed or whose job responsibilities no longer require access to the Provider Portal or to certain modules within it. The system requires entry of the User's employment termination date from the Provider Office, or the change in job responsibilities date, and the date that User's access to the Provider Portal is revoked or limited. If the date entered is greater than one (1) business day of the User's employment termination date, or change in job responsibilities date, the system shall generate a report for CalOptima's e-

Business Department detailing any areas of the Provider Portal that may have been accessed by the User, if any. The e-Business Department will review this audit report to determine whether a potential breach must be reported to CalOptima's Privacy Office.

4. Upon termination of a Provider Office in FACETS, all Providers and the Workforce connected to the Provider Office shall not be able to login to the Provider Portal.

N. Reinstatement of User accounts

1. Upon reinstatement of a Provider Office in FACETS, Provider Office Users connected to the Provider Office may regain access to the Provider Portal after completing account registration.

2. Provider Office Users whose access to the Provider Portal were previously revoked after being dormant for over sixty (60) calendar days may be reinstated after password reset.

IV. ATTACHMENT(S)

A. CalOptima Provider Portal User Agreement and Terms and Conditions of Use
B. Provider Portal User Training
C. CalOptima Provider Portal Access Agreement

V. REFERENCE(S)

A. CalOptima Policy HH.2022Δ: Record Retention and Access
B. CalOptima Policy HH.3002Δ: Minimum Necessary Uses and Disclosure of Protected Health Information and Document Controls.
C. CalOptima Policy HH.3020Δ: Reporting and Providing Notice of Security Incidents, Breaches of Unsecured PHI/PI or other Unauthorized Use or Disclosure of PHI/PI
D. CalOptima Policy IS.1303Δ: Audit, Review, Testing, and Change Management
E. CalOptima Policy IS.1601: In-House Provider Portal Administration and Support (Internal)
F. Title 45 Code of Federal Regulations (CFR), Part 164 - Security and Privacy, §§164.102 -164.534
G. Health Insurance Portability and Accountability Act (HIPAA) of 1996, Public Law 104-191

VI. REGULATORY AGENCY APPROVAL(S)

None to Date

VII. BOARD ACTION(S)

Date	Meeting
08/05/2021	Regular Meeting of the CalOptima Board of Directors

VIII. REVISION HISTORY

Action	Date	Policy	Policy Title	Program(s)
Effective	08/05/2021	IS.1600	Provider Access to In-House Provider Portal	Administrative

IX. GLOSSARY

Term	Definition
Access	Has the meaning given such term in Section 164.304 of Title 45, Code of Federal Regulations, i.e., the ability or the means necessary to read, write, modify, or communicate data or information or otherwise use any CalOptima system resource.
Administrative Safeguard	Has the meaning given such term in Section 164.304 of Title 45, Code of Federal Regulations. The administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's or business associate's workforce in relation to the protection of that information.
Authentication	Has the meaning given such term in Section 164.304 of Title 45, Code of Federal Regulations (i.e., the corroboration that a person is the one claimed).
Breach	The acquisition, access, Use, or Disclosure of protected health information in a manner not permitted under subpart E of 45 CFR Part 164 which compromises the security or privacy of the Protected Health Information. Breach excludes: (i) Any unintentional acquisition, access, or Use of Protected Health Information by a Provider Office or User, 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 45 CFR Part 164. (ii) Any inadvertent Disclosure by a User to another User authorized to access Protected Health Information at the same Provider Office, 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 45 CFR Part 164. (iii) A Disclosure of Protected Health Information where a Provider Office or User 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.
Corrective Action Plan (CAP)	A plan delineating specific and identifiable activities or undertakings that address and are designed to correct program deficiencies or problems identified by formal audits or monitoring activities by CalOptima, the State, or designated representatives. FDRs and/or CalOptima departments may be required to complete CAPs to ensure compliance with statutory, regulatory, or contractual obligations and any other requirements identified by CalOptima and its regulators.

Term	Definition
Covered Services	Means the following: • Those services provided in the Fee-For-Service Medi-Cal program (as set forth in Title 22, CCR, Division 3, Subdivision 1, Chapter 3, beginning with Section 51301), the Child Health and Disability Prevention program (as set forth in Title 17, CCR, Division 1, Chapter 4, Subchapter 13, Article 4, beginning with section 6842), and the California Children's Services (as set forth in Title 22, CCR, Division 2, subdivision 7, and Welfare and Institutions Code, Division 9, Part 3, Chapter 7, Article 2.985, beginning with section 14094.4) under the Whole-Child Model program effective July 1, 2019, to the extent those services are included as Covered Services under CalOptima's Medi-Cal Contract with DHCS ("Contract") and are Medically Necessary (as defined in the Contract), along with chiropractic services (as defined in Section 51308 of Title 22, CCR), podiatry services (as defined in Section 51310 of Title 22, CCR), speech pathology services and audiology services (as defined in Section 51309 of Title 22, CCR), and Health Homes Program (HHP) services (as set forth in DHCS All Plan Letter 18-012 and Welfare and Institutions Code, Division 9, Part 3, Chapter 7, Article 3.9, beginning with section 14127), effective January 1, 2020 for HHP Members with eligible physical chronic conditions and substance use disorders, or other services as authorized by the CalOptima Board of Directors, which shall be covered for Members notwithstanding whether such benefits are provided under the Fee-For-Service Medi-Cal program. • Those medical services, equipment, or supplies that CalOptima is obligated to provide to Members under the Centers of Medicare & Medicaid Services (CMS) Contract. • Those medical services, equipment, or supplies that CalOptima is obligated to provide to Members under the Three-Way contract with the Department of Health Care Services (DHCS) and Centers for Medicare & Medicaid Services (CMS).
Disclosure or Disclose	Has the meaning given such term in Section 160.103 of Title 45, Code of Federal Regulations, including the following: the release, transfer, provision of access to, or divulging in any manner of information outside of the entity holding the information.
Enterprise Administrator	An access role within Provider Portal designated to CalOptima staff residing in the Information Services, e-Business, or Provider Relations department responsible for: 1. Managing internal and external Provider Portal accounts; 2. Act as a point of contact to Local Office Administrators; and 3. Provide and terminate access to authorized staff for any Provider Office.
FACETS	Licensed software product that supports administrative, claims processing and adjudication, Membership data, and other information needs of managed care organizations.

Term	Definition
Health Care Operations	Has the meaning given such term in Section 164.501 of Title 45, Code of Federal Regulations including: activities including quality assessment and improvement activities, care management, professional review, compliance and audits, health insurance underwriting, premium rating and other activities related to a contract and health benefits, management and administration activities, customer services, resolution of internal grievances, business planning, and development and activities related to compliance with HIPAA.
HIPAA	The Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, which 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.
In-House	Developed and supported by internal CalOptima staff.
Local Office Administrator	A User at a Provider Office designated to: 1. Control CalOptima Link access; 2. Is the point of contact to CalOptima; and 3. Has the authority to provide and terminate access to authorized staff at the Provider's Office.
Member	A beneficiary enrolled in a CalOptima program.
Minimum Necessary	The standard which requires a covered entity to make reasonable efforts to limit the scope of the PHI it uses, discloses or makes a request for PHI to the minimum amount of PHI needed to accomplish the intended purpose. Minimum Necessary applies to internal uses of PHI, disclosures of PHI to external parties in response to a request and when Requesting PHI from another covered entity unless an exception under HIPAA applies (e.g. Minimum Necessary standard does not apply to treatment).
Payment	Has the meaning in 42 Code of Federal Regulations Section 164.501, including activities carried out by CalOptima such as: 1. Determination of eligibility, risk adjustments based on Member health status and demographics, billing claims management, and collection activities; 2. Review of health care services regarding medical necessity, coverage under a health plan, appropriateness of care, or justification of charges; and 3. Utilization review activities including pre-certification, preauthorization, concurrent, or retrospective review of services.
Principle of Least Privilege	The concept that all Users at all times should have as few privileges as possible, and access applications with as few privileges as possible to perform their work assignments.

Term	Definition
Protected Health Information	Has the meaning 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 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.
Provider(s)	A physician, nurse, nurse mid-wife, nurse practitioner, medical technician, physician assistant, hospital, laboratory, ancillary provider, health maintenance organization, or other person or institution that furnishes Covered Services.
Provider Office	For the purpose of this policy, a representation of one or more Providers participating in an office or as a group setting.
Provider Office Manager	For the purpose of this policy, an authorized representative of the Provider Office that manages the provider office and can confirm User employment for the Provider Office.
Provider Portal	CalOptima's information system which enables a Provider and/or a Provider Office and its Workforce to access Member health-related information to assist with Payment and Health Care Operations, not including CalOptima Link.
Provider Portal User Training	Required training module that must be completed by all Provider Portal Users prior to using the Provider Portal and no less than annually thereafter.
Restricted Information	Information that requires the highest level of access control and security protection, including, but not limited to, procedure and diagnosis codes related to treatment for HIV/AIDs, sexually transmitted or venereal diseases, family planning services, treatment for substance abuse and mental health issues or certain information related to minors or victims of abuse.
Sanction	An action taken by CalOptima, including, but not limited to, restrictions, limitations, monetary fines, termination, or a combination thereof, based on a First Tier, Downstream, and Related Entity's (FDR's) or its agent's failure to comply with statutory, regulatory, contractual, and/or other requirements related to CalOptima programs.
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.
Technical Safeguard	Has the meaning given such term in Section 164.304 of Title 45, Code of Federal Regulations. The technology, and the policy and procedures for its use, that protect electronic protected health information and control access to it.

Term	Definition
Unsecured Protected Health Information	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 PHI within an entity that maintains such information.
User	A person or entity with authorized access to the Provider Portal.
Violation	Violation means, as the context may require, failure to comply with an administrative simplification provision, as defined in 42 CFR Section 160.103.
Workforce	For the purposes of this policy, 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.