Policy:	GG.1659
Title:	**System Controls and Confidentiality of Provider Credentialing Information**
Department:	Medical Management
Section:	Quality Improvement - Credentialing
CEO Approval:	*/s/ Michael Hunn 12/16/2024*
Effective Date:	05/01/2021
Revised Date:	12/01/2024
Applicable to:	☒ Medi-Cal ☒ OneCare ☒ PACE ☐ Administrative

I. PURPOSE

This policy describes how CalOptima Health receives, stores, modifies, and secures Provider Credentialing information within the CalOptima Health Credentialing System as well as defines the scope of confidentiality for Credentialing files.

II. POLICY

A. CalOptima Health receives, stores, modifies, and secures all Credentialing information related to Provider in CalOptima Health's Credentialing System.

B. CalOptima Health electronically receives, dates, and stores the Primary Source Verifications (PSV) utilized in the Credentialing process within the Credentialing System.

C. The Credentialing System shall track and date Credentialing information when it is modified from its initial verification.

D. CalOptima Health shall determine the authorized staff who are authorized to review, modify, deactivate, and delete information in the Credentialing System, and circumstances appropriate for modification, deactivation, and deletion of information in accordance with Sections III.K-L. of this Policy.

E. Authorized CalOptima Health staff shall ensure that electronic credentialing information is kept confidential and stored in a secured Credentialing System that is password-protected, and access-restricted only to authorized staff, as follows:

1. CalOptima Health, its Health Network (HN) and First Tier, Downstream and Related Entities (FDRs) shall not have Practitioner and Organizational Provider (OP) Credentialing files be subject to disclosure under any conditions, except as required by law or as permitted by CalOptima Health policy.

    a. CalOptima Health shall be responsible for maintaining all Provider enrollment and credentialing documentation in a secure manner and location that ensures the confidentiality of each provider's personal information.

b. Provider enrollment records shall be made available upon request to the Department of Health Care Services (DHCS), Centers for Medicare & Medicaid Services (CMS), or other authorized governmental agencies.

c. CalOptima Health shall maintain the security and confidentiality of all of the information it receives from DHCS relating to the provider's high-risk designation and the results of the criminal background checks.

2. All Credentialing records shall be afforded all immunities, privileges, and protections available to "peer review bodies," as defined under California Business and Professions Code, Section 805.2, California Evidence Code, Section 1157, California Welfare and Institutions Code, Section 14087.58(b), and California Health and Safety Code, Section 1370.

3. Health care peer review and Quality Improvement records of CalOptima Health or a CalOptima Health committee shall not be subject to disclosure, except as required by law or as permitted by CalOptima Health Policy GG.1628: Confidentiality of Quality Improvement Activities, and this policy.

F. CalOptima Health shall have security controls in place, as described in Section III.H-I. of this Policy, to protect the information from unauthorized access and modification.

G. CalOptima Health shall ensure that the Credentialing System does not contain Member Protected Health Information (PHI) in accordance with Section II.H of this Policy.

H. CalOptima Health management and staff responsible for storing information in the Credentialing System or de-identifying Member PHI or conducting monitoring, audits, or oversight of such activities shall receive training as necessary and appropriate to carry out their respective responsibilities, including training on the following:

1. Information that qualifies as PHI;

2. Identifiers for PHI; and

3. CalOptima Health Policy HH.3019: De-identification of Protected Health Information (PHI), including compliance with Health Insurance Portability and Accountability Act (HIPAA) requirements for de-identification of PHI.

I. CalOptima Health shall audit the Credentialing System to ensure:

1. PSV information is received, dated, and stored;

2. Information that is modified is tracked and dated from its initial verification;

3. Only authorized staff review, modify, deactivate, and delete information, and only in circumstances when modification, deactivation, or deletion is appropriate; and

4. Security controls are in place to protect information from unauthorized modification.

J. CalOptima Health shall ensure that downstream systems and databases are consistent with verified Credentialing data, including education, training, board certification, and specialty.

III. PROCEDURE

A. CalOptima Health will obtain, review, and store PSVs within the Credentialing System's practitioner file and Credentialing record, as specified in CalOptima Health Policy GG.1650: Credentialing and Recredentialing of Practitioners, such as:

   a. Practitioner state license number;

   b. Practitioner Drug Enforcement Agency (DEA) identification number;

   c. Practitioner Type 1 National Practitioner Identification (NPI) number;

   d. Practitioner's credentialing approved specialty and/or subspecialty;

   e. Practitioner's Taxonomy Code issued to align with credentialed specialty;

   f. Physician board certification(s) and board certification status(es);

   g. Mid-level practitioner supervising Physician;

   h. Physician hospital affiliation(s) and status;

   i. Malpractice/Professional Liability Insurance; and

   j. Credentialing decisions made by the Credentialing and Peer Review Committee (CPRC).

B. CalOptima Health will obtain, review, and store PSVs within the Credentialing System's OP file and credentialing record, as specified in CalOptima Health Policy GG.1651: Assessment and Reassessment of OPs, such as:
   1. State or Business License;

   2. Accreditation;

   3. Type 2 NPI;

   4. Taxonomy/Specialty; and

   5. Credentialing decisions made by the CPRC.

C. During the credentialing process or between credentialing cycles, electronic sources of PSVs and monitoring of Provider information may be utilized, including:

   1. Public or private websites or portal of issuing body and/or contracted entity used for displaying issuing body's verification data;

   2. Integrated data sources which operate in conjunction with Credentialing System, such as:

      a. State License monitoring;

      b. Drug Enforcement Agency (DEA) monitoring;

      c. National Practitioner Data Bank (NPDB);

      d. Physician Board Certifications; and/or

e. Office of Inspector General (OIG).

3. Official published listings made available to CalOptima Health from either government entities or issuing bodies; or

4. Other internal sources used for determining Credentialing decisions.

D. Upon receipt of PSVs, the Credentialing staff shall review and upload data into the Credentialing System. The Credentialing System shall electronically record the date of the verification and the person who performed the verification.

1. If the Credentialing staff finds any errors or omissions on any document submitted by Provider, the Credentialing staff will request a new or revised document from the Provider.

E. If the Credentialing staff identifies primary source data that requires updating between credentialing cycles, Credentialing staff will update the Provider file in the Credentialing System and the modified information will be tracked and dated within the system.

F. CalOptima Health shall ensure only authorized employees have access to the building and Credentialing department by limiting physical access in accordance with GA.4000: Physical Security and Access Controls which include:

1. Physical safeguards such as locked doors, signs warning of restricted areas, surveillance cameras, alarms;

2. Personnel controls such as identification badges, visitor badges, and escorts; and

3. Private security or patrol for the facility.

G. CalOptima Health shall ensure electronic media, storage devices and hardware are monitored and recorded for movement in and out of the facility in accordance with ITS.1102: Technical Safeguards - Electronic Media, Storage Devices and Hardware Controls.

H. CalOptima Health shall ensure Credentialing Systems are locked and users are logged-off when not in use per policy ITS.1201: Technical Safeguards - Access Controls.

I. The Credentialing System and Provider Files are cloud-based therefore credentialing information will be secured with no physical access to credentialing information in accordance with CalOptima Health Policy ITS.1201: Technical Safeguards - Access Controls.

1. Access to Credentialing information will be based on authentication of unique user identity by ensuring credentials entered upon log-in match those stored in the system. Once properly authenticated, CalOptima Health shall grant user authorized access to perform credentialing functions.

2. Appropriate controls will be implemented based on User Group Security. User Group Security will be approved and authorized by Credentialing Management and implemented by the System Administrator.

3. Credentialing staff will be required to use strong passwords, avoid writing down passwords, use different passwords for different systems, use Identifications (ID) and passwords unique to each user, and will change passwords when requested by staff or if passwords are compromised.

a. Passwords are to be at least eight (8) characters and shall include:

i. At least one (1) number;

ii. At least one (1) letter; and

iii. At least one (1) special character.

b. Passwords are to be changed every 60 calendar days.

c. Passwords will be disabled or removed when employees leave the Credentialing department or organization.

4. For those users separating with CalOptima Health, their access is automatically set to expire on their last day of work, based on the information documented in the Human Resources system within the individuals last day. There is logic built between these two systems so that this happens automatically based on the information documented in the HR system in accordance with CalOptima Health Policy ITS.1301: Security Awareness Training.

J. User Group Security shall be based on user functional roles and is established by the System Administrator. The System Administrator will maintain User Group Security within the Credentialing System.

1. CalOptima Health Credentialing staff, which includes Credentialing Program Assistant, Credentialing Coordinators, and Credentialing Auditors, are authorized to enter, modify, and deactivate Provider files in the Credentialing System, per User Group Security. Modifications to primary specialty in the Provider file, modifications to credentialing record after a decision is made, and deactivations as a result of record closure or administrative term require Credentialing Management approval.

2. Credentialing Management staff are authorized to enter, modify, and deactivate Provider files in the Credentialing System, per User Group Security. Modifications to primary specialty in the Provider file, modifications to Credentialing record after a decision is made, and deactivations as a result of record closure or administrative term will be reviewed, documented, and approved by Credentialing Management.

3. System Administrators have read-only access and are only authorized to delete records in the Credentialing System upon e-ticket request by Credentialing Management.

K. All modifications and deactivations made within the Credentialing System will be tracked in the contact log and audit log, including:

1. Date the information was modified or deactivated;

2. Staff who made the modification or deactivation, and the value in the field prior to the edit; and

3. Supporting documentation for how and why the modification was made.

L. Appropriate reasons for modifications of a Provider file by Credentialing staff include:

1. Update to demographic information upon notification from a Provider.

2. Update to Board Certification, DEA and insurance certificates as they expire.

3. Update to Sanction Information as released by sanction entities.

4. Correction identified during Credentialing process, in the Credentialing record, prior to the credentialing decision.

5. Correction identified after a credentialing decision, with Credentialing Management approval.

6. Modification of primary specialty with Credentialing Management approval.

7. Modifications to remove PHI if identified with the Provider file.

M. Appropriate reasons for deactivations of a Provider file by Credentialing staff include:

1. Incomplete initial Credentialing applications.

2. Corrections to a credentialing file (i.e., change of insurance carrier, updates to license or DEA requiring a deactivation of the old information once new information is entered).

3. Record closure of a credentialing file, with Credentialing Management approval.

4. Termination of a Provider with Credentialing Management approval.

N. All deletions of records within the Credentialing System will be submitted by Credentialing Management via e-ticket system to System Administrator. The System Administrator will implement the deletion, and will track:

1. Date the information was deleted;

2. Staff who made the deletion; and

3. Supporting documentation for how and why the deletion was made.

O. Appropriate reasons for deletions by the System Administrator include:

1. Credentialing information attached to the wrong Provider file.

2. Duplicate Provider file was created.

P. Auditing and Monitoring

1. The Credentialing Auditor shall audit the credentialing system at least Annually, utilizing a statistically valid sample of Provider files and audit logs within the Credentialing System. The Audit would include:

a. The review of Primary source Verification information that is received, dated, and stored in the system;

b. The review of audit logs for recredentialing dates, which show when, how and who modified the dates from its initial verification;

c. The review of audit logs and tasks system to ensure authorized staff who review, modify, deactivate, and delete information, and only in circumstances when modification, deactivation or deletion is captured;

d. At least on an annual basis, the Credentialing Auditor shall conduct a review of all active user accounts within the credentialing system. The review includes active employment status, title/role, and business need for accessing credentialing records;

e. The Credentialing Auditor will perform a quality review of a report for all modifications to the credentialing files. The findings will be presented at the Credentialing Committee at least annually;

f. At least on an annual basis, the Credentialing Auditor shall conduct a qualitative and quantitative analysis of the findings from the quality review; and

g. If the Credentialing Auditor identifies any modifications that did not meet the established policy, the Credentialing Manager shall identify remediation steps to address noncompliant findings and a quarterly monitoring process will be set in place until it demonstrates improvement for one finding over at least three consecutive quarters.

2. The Credentialing Auditor shall annually require all Credentialing staff to attest to security controls that are in place to protect information from unauthorized modification which include use of strong passwords, avoid writing down passwords, using different passwords for different accounts, use IDs and passwords unique to each user, and changing passwords if they feel their password has been compromised.

a. The Credentialing Auditor , at least on annual basis, shall monitor attachments (*i.e.*, copies of original records) that required de-identification under this Policy to ensure that Member PHI has been properly de-identified, in accordance with CalOptima Health Policy HH.3019: De-identification of Protected Health Information (PHI), and permanently removed by trained staff prior to storage in the Credentialing System.

3. At least annually, the Audit & Oversight (Internal) Department, shall perform oversight of the audit and monitoring process in accordance with CalOptima Health Policy HH.4002: CalOptima Health Internal Oversight.

Q. Approved CalOptima Health, HN and other FDR staff shall ensure that Credentialing files are kept confidential by electronically storing them in a secure manner, password-protected, and access-restricted only to authorized employees.

R. Physical copies of Credentialing files shall not be left unattended in open office areas including, but not limited to, staff workstations, printer stations, and common areas accessible to staff.

S. All members of the Credentialing and Peer Review Committee (CPRC) are required to sign confidentiality statements on an annual basis.

T. Auditors, including but not limited to external consultants, are required to sign confidentiality statements prior to Credentialing audits.

U. All credentialing files are considered sensitive in content and shall be available for review only by those granted access and/or when distributed to the committee. All copies of the minutes are collected and destroyed at the conclusion of the meeting.

IV. ATTACHMENT(S)

Not Applicable

V. REFERENCE(S)

A. NCQA Credentialing Standards: Practitioner Credentialing Guidelines and Credentialing System Controls
B. CalOptima Health Policy GA.4000: Physical Security and Access Controls
C. CalOptima Health Policy GG.1628: Confidentiality of Quality Improvement Activities
D. CalOptima Health Policy GG.1650: Credentialing and Recredentialing of Practitioners
E. CalOptima Health Policy GG.1651: Assessment and Reassessment of Organizational Providers
F. CalOptima Health Policy HH.3019: De-identification of Protected Health Information (PHI)
G. CalOptima Health Policy HH.4002: CalOptima Health Internal Oversight
H. CalOptima Health Policy ITS.1102: Technical Safeguards - Electronic Media, Storage Devices and Hardware Controls
I. CalOptima Health Policy ITS.1201: Technical Safeguards - Access Controls
J. CalOptima Health Policy ITS.1301: Security Awareness Training
K. California Business and Professions Code, §805.2
L. CalOptima Health Contract with the Centers for Medicare & Medicaid Services (CMS) for Medicare Advantage
M. CalOptima Health Contract with the Department of Health Care Services (DHCS) for Medi-Cal
N. CalOptima Health PACE Program Agreement
O. Credentialing and Peer Review Committee Description
P. NCQA Health Plan Standards and Guidelines: Credentialing
Q. California Evidence Code, §1157
R. California Health and Safety Code, §1370
S. California Welfare and Institutions Code, §14087.58(b)

VI. REGULATORY AGENCY APPROVAL(S)

Date	Regulatory Agency	Response
11/09/2022	Department of Health Care Services (DHCS)	File and Use

VII. BOARD ACTION(S)

None to Date

VIII. REVISION HISTORY

Action	Date	Policy	Policy Title	Program(s)
Effective	05/01/2021	GG.1659	System Controls of Provider Credentialing Information	Medi-Cal OneCare OneCare Connect PACE
Revised	12/31/2022	GG.1659	System Controls of Provider Credentialing Information	Medi-Cal OneCare PACE
Revised	10/01/2023	GG.1659	System Controls of Provider Credentialing Information	Medi-Cal OneCare PACE
Revised	02/01/2024	GG.1659	System Controls of Provider Credentialing Information	Medi-Cal OneCare PACE
Revised	12/01/2024	GG.1659	System Controls of Provider Credentialing Information	Medi-Cal OneCare PACE

IX. GLOSSARY

Term	Definition
Credentialing	Medi-Cal: The process of determining a Provider or an entity's professional or technical competence, and may include registration, certification, licensure and professional association membership. OneCare: The process of obtaining, verifying, assessing, and monitoring the qualifications of a practitioner to provide quality and safe patient care services. PACE: The recognition of professional or technical competence. The process involved may include registration, certification, licensure, and professional association membership.
Credentialing and Peer Review Committee (CPRC)	The Credentialing and Peer Review Committee makes decisions, provides guidance, and provides peer input into the CalOptima Health provider selection process and determines corrective action necessary to ensure that all Practitioners and providers who provide services to CalOptima Health Members meet generally accepted standards for their profession in the industry. The CPRC meets at least quarterly and reports to the CalOptima Health Quality Improvement (QI) Committee.
Credentialing Management	Credentialing Management includes Credentialing Supervisor, Quality Improvement Manager, and Quality Improvement Director.
Credentialing System	Database used for Credentialing activities which captures and stores credentialing information. The Credentialing System creates Provider files for each unique provider and creates Credentialing records for each Credentialing cycle.
Downstream Entity	Any party that enters into a written arrangement, acceptable to DHCS and/or CMS, with persons or entities involved with a CalOptima Health Program benefit, below the level of arrangement between CalOptima Health and a First Tier Entity. These written arrangements continue down to the level of the ultimate provider of both health and administrative services.
First Tier, Downstream, and Related Entities (FDR)	Means First Tier, Downstream or Related Entity, as separately defined herein. For the purposes of this policy, the term FDR includes delegated entities, contracted providers, Health Networks, physician groups, Physician Hospital Consortia, and Health Maintenance Organizations
First Tier Entity	Any party that enters into a written arrangement, acceptable to DHCS and/or CMS, with CalOptima Health to provide administrative services or health care services to a Member under a CalOptima Health Program.
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.
Member	A beneficiary enrolled in a CalOptima Health Program.
Modify	To make any changes to a data element within a field in the Credentialing System, which would include updating or correcting Provider credentialing information.

Term	Definition
Organizational Provider	Medi-Cal: Hospitals, Intermediate Care Facilities (ICF), Intermediate Care Facilities for the Developmentally Disabled (ICF/DD), Intermediate Care Facilities for the Developmentally Disabled-Nursing (ICF/DD-N), Intermediate Care Facilities for the Developmentally Disabled-Habilitative (ICF/DD-H), Skilled Nursing Facilities (SNF), sub-acute facilities-adult, sub-acute facilities-pediatric, home health agencies, extended care facility, nursing home, free-standing surgical center, seating clinic, urgent care centers, radiology facilities, laboratory facilities, pathology facilities, and Durable Medical Equipment (DME) vendors. OneCare: Organizations or institutions that are contracted to provide medical services such as hospitals, home health agencies, nursing facilities (includes skilled nursing, long term care, and sub-acute), free standing ambulatory surgical centers, hospice services, community clinics including Federally Qualified Health Centers, urgent care centers, End-Stage renal disease services (dialysis centers), Residential Care Facility for the Elderly (RCFE), Community Based Adult Services (CBAS), durable medical equipment suppliers, radiology centers, clinical laboratories, outpatient rehabilitation facilities, outpatient physical therapy and speech pathology providers, diabetes centers, and portable x-ray suppliers.
Physician	A licensed practitioner including, but not limited to, a Doctor of Medicine (MD), Doctor of Osteopathy (DO), Doctor of Podiatric Medicine (DPM), Doctor of Chiropractic Medicine (DC), Doctor of Dental Surgery (DDS), furnishing covered services.
Primary Source Verification (PSV)	Medi-Cal: Verbal or written information received directly from the issuing source. OneCare: The process by which a Health Network or sub-delegated entity verifies Credentialing and Recredentialing information from the organization that originally conferred or issued the Credentialing element to the Practitioner.
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.

Term	Definition
Provider	Medi-Cal: Any individual or entity that is engaged in the delivery of services, or ordering or referring for those services, and is licensed or certified to do so. OneCare: Any Medicare provider (e.g., hospital, skilled nursing facility, home health agency, outpatient physical therapy, comprehensive outpatient rehabilitation facility, end-stage renal disease facility, hospice, physician, non-physician provider, laboratory, supplier, etc.) providing Covered Services under Medicare Part B. Any organization, institution, or individual that provides Covered Services to Medicare members. Physicians, ambulatory surgical centers, and outpatient clinics are some of the providers of Covered Services under Medicare Part B.
Related Entity	Any entity that is related to CalOptima by common ownership or control and that: performs some of CalOptima'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 at a cost of more than $2,500 during a contract period.
System Administrator	The individual who is the administrator for the Credentialing System and is responsible for managing User Group Security and Credentialing System configuration. This function will be assigned to IS Department – Application Management.
User Group Security	A set of user security rules, based on user role and function.