Policy and Procedure No: CR 7.3	**Revision No: 3**
Division: Care Management	
Department: Credentialing	
Title: PHC-CA Credentialing System Controls	
Effective Date: 9/1/2021	
Supersedes Policy No: CR 7.0, CR 7.1, CR 7.2	
Reviewed/Revised by: Renee Barker	**Review/Revision Date: 12/16/2025**
Approving Committee: Credentialing Committee	**Date: 12/16/2025**
Executive Oversight Committee Date: 12/16/2025	

Purpose:

PHC California (the Health Plan) has and maintains an electronic credentialing file and a physical file for each practitioner applying for participation in the Health Plan. The credentialing file includes both a data and document component. The Health Plan uses the CACTUS credentialing software which houses data elements of primary source verification including demographics, education, license, certification, hospital and insurance information. The document management system houses images of the credentialing application, correspondence related to credentialing and all primary source verifications.

Policy:

It will be the policy of the credentialing program to determine the following credentialing process:

1. How primary source verification is received, dated and stored.

2. How modified information is tracked and dated from its initial verification.

3. Staff who are authorized to review, modify and delete information, and circumstances when modification or deletion is appropriate.

4. The security controls in place to protect the information from unauthorized modification.

5. How the organization audits the processes and procedures.

Procedure:

A. Primary Source Verification information: The Health Plan process for receiving, storing, reviewing, tracking and dating credentialing information complies with accreditation, regulatory, state and customer requirements, as applicable and reflects the Information Technology measures designated to maintain data integrity and security.

   1. Credentialing information is received and stored electronically from several sources, including but not limited to:

      a) Provider via fax (e-Fax stored electronically);

      b) Screen printed or downloaded from Primary or Secondary Source;

      c) Downloaded from CAQH (Council for Affordable Healthcare.); and

      d) Secure email.

2. Internet and electronic verifications must include the date generated by the source when the information is retrieved. If the source report does not generate a date, the Health Plan uses the date noted in the credentialing file by the Credentialing Specialist staff person who verified the credentials. Internet verifications must include the URL.

3. The Credentialing Specialist must clearly document all verbal verifications in writing indicating the name of the person providing the verification, and the organization or institution the person is representing.) in the header, footer or clearly identify the source of the verification.

4. Written verifications in the form of letter or cumulative report must include the date of the official document (date on the letter or report), not the receipt date, to assess performance against timeliness requirements. Where applicable, Credentialing Specialist must obtain the latest cumulative report and periodic updates released by the approved source.

5. Primary source verification data and documentation are uploaded to their respective files and are tracked and dated within the application.

6. All data and documents uploaded and input to the credentialing applications are tracked with the following elements:

    - Creation date
    - Last modified date
    - Created user

Data and documentation that is stored in the CACTUS credentialing software and document storage is reviewed for quality and accuracy during the credentialing and re-credentialing process. Data in the credentialing software is regularly audited between credentialing cycles in the form of various data integrity reports and queries. Erroneous data is corrected in the application as it is identified to ensure credentialing data is correct and up to date.

B. Tracking Modifications

    1. In order to maintain an accurate credentialing file, modification to data and documentation may be required. The Health Plan Credentialing Specialist will complete updates during credentialing and re-credentialing process, as deemed necessary. The Credentialing Specialist will also update information between credentialing cycles to correct erroneous data or update expired verifications. Any modifications to credentialing data and documentation will be tracked.

    2. When credentialing information is modified the Credentialing Department will use the audit log that tracks the last modified date when a date field is changed.

    3. How information is modified - utilize audit log to track the old value and new value clearly identifying how the data was modified, who made the modification. The Health Plan utilizes audit logs to track the user who made modification.

C. Authorization to modify information: System access is requested and granted on an as needed basis and audited to ensure appropriateness.

1. IP access is limited to users who have been identified by supervisory staff as needing to use the application as part of their job functions.

2. The following Credentialing staff can access, modify, or delete information:

    - Manager of Credentialing
    - Director of Credentialing

3. If the Credentialing Specialist needs to modify or delete then they need to contact the authorized users referenced above.

D. **Securing Information**

1. The Credentialing department adheres to the Health Plan information, physical or electronic, to be secured where access is restricted. Computers must be locked or logged off while unattended. Individuals must remove documents containing confidential information from printers and fax machines immediately and not leave unattended.

2. Employees granted access to credentialing data and documents management systems require both a user ID and password. To gain access to either system the user must enter their unique ID and password. Once logged in, the user may use windows authentication over the corporate network to log in going forward.

E. **Credentialing Audit Process**

The completed credentialing files undergo an audit process by random sampling. A report is generated each month listing the provider credentialing files that are processed, completed and approved by the credentialing committee. On a monthly basis, the credentialing lead/manager reviews at least 10% of the files completed and chooses the files randomly. An audit tool (based on NCQA/state standards) is used to determine whether the files are compliant with all required elements.

Definitions:

1. CAQH: Council for Affordable Quality Healthcare

2. NCQA: National Committee for Quality Assurance

Monitoring:

This policy is updated as often as necessary, reviewed, and approved at least annually by the Credentialing and Peer Review Committee.

Reference(s):

NCQA: CR 1 Element C