DEPARTMENT: ~~Corporate~~ Credentialing	**DOCUMENT NAME:** Credentialing System Controls
PAGE: Page 1 of 6	**REPLACES DOCUMENT**:
APPROVED DATE:	**RETIRED:**
EFFECTIVE DATE: 03/01/2022	**REVIEWED/REVISED:** ~~39~~/~~15~~/2022
PRODUCT TYPE: ALL	**REFERENCE NUMBER:** ~~CC~~LA.CRED.13

SCOPE:
Louisiana Healthcare Connections (LHCC also known as the "MCO")~~Corporate and Plan~~ Medical Management, Provider Relations and Credentialing Departments

PURPOSE:
To ensure that system controls are in place to monitor modifications to credentialing records.

POLICY:
~~Centene~~ LHCC has established procedures for monitoring modifications to credentialing records including but not limited to:

- How primary source verification (PSV) information is received dated and stored
- How modified information is tracked and dated from its initial verification
- Titles and Roles of Staff Authorized to review, modify and delete credentialing information, and circumstances when modification or deletion is appropriate
- Security controls in place to protect credentialing information from unauthorized modification

At least annually, ~~Centene~~ LHCC monitors compliance with credentialing system controls and takes appropriate action, when applicable by:

- Identifying modifications to credentialing records that are done for reasons other than allowed. Analyzing instances of modifications that do not meet Centene's policy for modifications
- Acting on all findings and implementing a quarterly monitoring process until there has been improvement over three (3) consecutive quarters.

PROCEDURE:

1. PSV Information
    a. Received – through approved primary and secondary sources including but not limited to web, mail and phone
    b. Reviewed – automatic recording of date verified and name of the staff conducting review of credentials in the credentialing database (CenProv)
    c. Tracked – via the credentialing database (CenProv)

d. Dated – automatic recording of date verified and name of the staff conducting review of credentials in the credentialing database (CenProv)
e. Stored – through the credentialing database and written to the document repository where files cannot be modified or deleted (CenProv/FileNet)

2. Tracking and Modification of Credentialing Information

Modified Information is tracked, dated and stored in the credentialing database (CenProv). An audit log is recorded by the system as the credentialing file moves through the process. The audit log can be viewed during any step of the process to view when data was either entered, modified, or removed from the visible file. Audit log information includes dates/time, what information was modified, why the information was modified and the user who performed the modification. Modification or deletion of credentialing information is not permitted by the credentialing database (CenProv) in any way after the decision has been logged. Once documents are attached in the credentialing database (CenProv), they are written to the document repository (FileNet) where they cannot be modified or deleted. Modification or deletion of credentialing information is allowable in the following circumstances, but is not limited to:

a. During the normal credentialing and re-credentialing process per Centene Corporation credentialing policy (~~CC~~LA.CRED.01)
b. If Credentialing staff receives information from NCQA-approved primary source institutions regarding correction and or updates to information provided to ~~Centene Corp~~Provider Data Management Department (PDM).
c. If Credentialing staff receives notice from the NPDB that a report has been revised or deleted.
d. If MCO is notified by the provider or Plan of changes to provider credentialing status such as a request to be termed from the MCO.

3. Authorization to Modify Credentialing Information

a. ~~Frontline credentialing staff~~ Credentialing Specialist I, Credentialing Specialist II and Lead Credentialing Specialist are permitted to update/modify information necessary during the normal credentialing and re-credentialing process. These credentialing staff members perform credentialing and recredentialing activities according to plan specifications and in compliance with NCQA standards including but not limited to:

i. Maintaining and updating the credentialing database
ii. Communicating with physicians, office managers, providers and other third parties to secure needed credentialing information
iii. Processing, tracking and filing credentialing applications within established standards
iv. Responding to internal and external inquiries regarding credentialing status of a provider or group
~~i.~~v. Assisting with coordination of the credentialing committee

b. The credentialing database does not allow modification and/or deletion of any data after a decision has been logged due to workflow order of operations in the credentialing system.
c. The following staff are authorized to create and cancel cases which store credentialing information prior to decision:
    i. Credentialing Supervisor, Manager or above

4. Securing Information
    a. Credentialing information is stored, modified and secured in a ~~Centene Corporation~~ PDM private server based stable and controlled credentialing database. The credentialing system has controls in place to ensure the security of information and that it is protected from unauthorized access. CenProv software access is initiated by a user via a software request ticket and approved or denied for installation by management and the Plan's IT department. Accounts to CenProv are role based and password protected. Only authorized users are able to gain access to the database and are given write or read only access based on the user's role within the Organization.
    b. Physical access to ~~Centene~~ PDM servers is restricted to authorized users per PDM's Centene Corporation Physical Security Policy (CC.SECR.11.1) and the Physical Security Standard (CC.SECR.11.1.A).
    c. Password Protection
    User accounts and access rights in CenProv are as follows:
    - System Users [Desktop users] – Read only
    - System Users [Triage/Maintenance] – Read and write only
    - System Users [Credentialing & Delegation Specialist] – Write only and selected query access
    - Systems Users [Supervisor & Manager] – Read, write, cancel and all query access
    - Systems Administrators – all system functions

Password protection and minimum password standards are outlined in Centene Corporation's System and Application Access and Password Standards Policy (CC.SECR.9.4.A).

d. Modification after a decision has been made is not permitted due to workflow order of operations in the credentialing system. Once documents are attached in the credentialing system, they are written to the document repository where they cannot be modified or deleted at any point.
e. Credentialing Supervisors, Managers, and System Administrators are the only authorized users able to delete information from the credentialing database prior to a decision. Input of and access to electronic credentialing information and documentation is undertaken by appropriate individuals via individual login and individually determined password. This limits physical access to the electronic credentialing information and documentation maintained in the ~~Plan's~~ MCO's database (CenProv).

5. Credentialing System Controls Oversight/Audits
    a. Identification of Credentialing Record Modifications
        i. Oversight of modifications performed within the credentialing database (CenProv) are reviewed by the Corporate Center of Excellence (COE) team within Provider Data Excellence. The auditor completes a ~~semi~~ annual audit to review information that has been modified or deleted, who made the modification/deletion, were modifications/deletions made by account users authorized to do so, and was the modification/deletion made for one of the acceptable reasons.
        ii. Sampling methodology is as follows:
            1. The COE Auditor will pull a file universe of practitioner cases with modifications during the reporting timeframe.
            2. The COE Auditor determines the sample selection size of 5% or 50 files, whichever is less from the entire universe of files. The sample of files to be audited will only include files with a modification(s). File sample universes and samples are drawn at the individual health plan level.

a. At a minimum, the audited sample should include 10 modified initial credentialing files and 10 modified recredentialing files with a modification(s). If there are less than 10 cred or 10 recred files during the monitoring period for ~~an individual health plan~~the MCO, all of the applicable cred or recred files with modifications during the monitoring period will be assessed.

3. The COE Auditor will run an audit log of each file to determine why, when and what information was modified or deleted and confirm an authorized user performed the modification or deletion for an appropriate reason as outlined in this policy and document their findings for each file.
4. The COE Auditor will report any discrepancies identified/modifications performed that are not allowed per this policy to the Credentialing Manager and/or Director.
5. The Credentialing Manager and/or Director will immediately address the discrepancies with the Credentialing Specialist.
6. If needed, ~~T~~the credentialing system will be updated to reflect correct data.
7. The COE Auditor will analyze modifications performed for reasons not allowed according to ~~Section 2.a-f of~~ this policy.
    a. The COE Auditor will conduct qualitative and quantitative analysis of the audit results.
    b. The report will include the number or percentage of files with modifications that do not meet policy expectations.

iii. Actions Taken to Address Findings/Opportunities:

1. If findings are present, the COE Auditor will proceed with a quarterly monitoring process to assess effectiveness of actions until improvement of at least one finding is demonstrated over three consecutive quarters.
2. Oversight is provided by the Credentialing Manager and/or Director who reviews the final audit report.

3. The Credentialing Manager and/or Director will take action to address any findings/opportunities identified by the qualitative and quantitative analysis including, but not limited to:
    a. Routine scheduled monthly monitoring with staff responsible for actions.
    b. ~~Centene Corporation~~PDM will monitor all opportunities until improvement has been achieved over three consecutive quarters.