


No. CD-1016	Credentialing System Controls	
Effective Date: 01/01/2020	POLICY AND PROCEDURE	
Committee Approval: 10/14/2022 Previous Versions: See revision history on last page		
NCQA Standard: CR 1C Credentialing System Controls		

I. SCOPE

This policy applies to Canopy Health, its delegated Medical Groups/IPAs and any other entity or organization with which Canopy Health contracts to perform provider credentialing on Canopy Health’s behalf (each a “Contractor”). To the extent that any delegate or Contractors perform functions set forth herein, references to “Canopy Health” or the “Credentialing Department” shall be interpreted to refer to such Contractors.

II. PURPOSE

The purpose of this policy is to have systems or process in place for storing, modifying and securing credentialing information.

III. DEFINITIONS

Credentialing: The process by which Canopy Health evaluates providers prior to contracting said providers to render services to members. Eligibility for network participation is determined by the extent to which applicants meet defined requirements for education and training, licensure and certifications, professional standing, service availability and accessibility, and quality requirements. **Attestation:** The statement which attests to the validity of information contained in the application and releases Canopy Health to obtain primary source verifications.

Credentialing Peer Review Committee: A group of providers selected by Canopy Health that evaluate the qualifications and make the final determination regarding the status of providers applying for participation in Canopy Health’s network, and evaluate the necessity, quality or utilization of care rendered by providers in the network. Peer review is conducted by other health care providers from the same discipline or with similar or essentially equal qualifications who are not in direct economic competition with the health care professional under review.

Participating Provider: Any practitioner or organization that is contracted or employed by Canopy Health to render services to members.

IV. POLICY

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

- A. How primary source verification is received, dated and stored.
- B. How modified information is tracked and dated from its initial verification.
- C. Staff who are authorized to review, modify and delete information, and circumstances when modification or deletion is appropriate.
- D. The security controls in place to protect the information from unauthorized modification.
- E. How the organization audits the processes and procedures in factors A-D

V. PROCEDURE

A. Primary source verification information

Credentialing applications and supporting documents are received via the following: electronically (CAQH), mail or email. The applications/documents are reviewed by the credentialing staff, dated and tracked electronically and manually via a checklist. Upon completion of the credentialing process, these documents are stored in a department drive and in the credentialing database of which access are limited to the credentialing and authorized company staff.

B. Tracking Modifications

Modifications are applicable if there are updates to the applications and/or supporting documents which are logged through the checklist or electronically through the database. The database is able to identify the date the change was made and the person who made the updates or modifications. Updates on the checklist only shows the most recent change or modification. However, copies of the previous and recent modifications/updates are combined in the provider's file with the checklist. These documents are electronically saved in the department drive and the credentialing database.

The credentialing staff is responsible for the modification of the information on the credentialing application and/or supporting documents. If modifications are done manually, the staff initials the updates with the date the change was made. If modifications are done electronically, the database shows the date it was modified and name of staff and what change was made.

C. Authorization to modify information and to secure information

Credentialing staff are assigned user roles based on areas of responsibility as defined in their job description. Each user role is assigned specific read/write system access as needed to perform their duties which may include modifying and deleting information.

System Administrator/Credentialing Manager/Director may allow the Credentialing staff (Credentialing Specialist/Coordinator) to create new files and records, make changes in existing files/records, delete existing files/records, grant the right to create field specific notes, right to change the file properties setup, allow change to the order in which a list is displayed, allow access to the audit log viewer and enable the use of imaging with the file. The System Administrator/Credentialing Manager/Director can also grant access just to view rather than grant access rights depending on the need.

Verification information may be modified by Credentialing Specialists, Supervisors or Managers when verification information changes – examples include but are not limited to (see below). If credentialing information changes, new verifications will be obtained, initialed/dated by Credentialing Staff, and stored in the applicant's credentialing hard file and/or electronic file.

Appropriate modifications to the credentialing information may include but not limited to the following:

- Updates to expired licensure or other documents
- Changes/updates to education, training, or privileges
- To correct data entry errors
- Duplicate profiles
- Documents appended to incorrect provider profile

Inappropriate modifications may include but not limited to the following:

- Altering credentialing approval dates
- Altering dates on verifications
- Whited out dates or signatures on hard copy documents
- Unauthorized deletion of provider files or documentation

Access to this drive is only available to the credentialing staff and authorized personnel. Files are also saved electronically via the credentialing database. Access to these files/documents are password protected. Each user is assigned an ID and password to log in to the database. A database administrator sets security policies of users logging into the database such as password age, length, lockout threshold, password complexity and password encryption. Passwords must be changed at least once every 90 days. Files are scanned and saved in a

department drive and backed up every night to a server. Access to the credentialing database (Visual Cactus) is granted with the process below:

- Users are required to submit an eID request form on <https://icon.coniferhealth.com> to request access to Visual Cactus
- The eID goes through several different approvals (Management approvals and Security Administrator approval) to ensure correct access is being approved.
- Once all the approvals are completed, the request is forwarded to the VBC Support desk to create Visual Cactus account.
- Access is granted based on the requester's job title. Visual Cactus Security access profiles are available for each job title to ensure users have access to only the modules that they're required to work in.
- Company Access profile' security option is used to restrict a user's access to a specific company or set of companies only.

For access to Visual Cactus (credentialing database), there are 5 different access levels for each function. See below:

- No Access
- Read Only
- Read/Write
- Read/Write/Delete
- Special Access

The credentialing staff are the only ones who are able to access, update, modify and delete the credentialing information electronically. Deletion is only allowed when information needs to be updated and/or information is incorrect for the provider. Levels of access are assigned through user groups. A user group may consist of a single user or multiple users with responsibilities assigned.

To the extent permitted by the device or Software system, parameters for User-chosen Passwords or passphrases are the following:

1. Contain at least eight (8) characters.
2. Contain both alpha and numeric characters (letters and numbers).
3. Contain at least one lower case and one upper case alphabetic character.

There are rules to follow to be able to not use passwords that would be easy to guess or crack which are as follows:

1. Passwords or passphrases that are identical or substantially similar to the UserID to which it is assigned;
2. Passwords or passphrases that are identical or substantially similar to Passwords used within a twelve (12) month period.

3. Any part of your name, a spouse's name, or children's names;
4. Any part of your street address (street, town, house number, zip code) or your home, work, pager or cell phone numbers;
5. Any of your family's Social Security Numbers or birth dates;
6. Single words found in a dictionary, including proper names, geographical locations, common acronyms, and slang (computer programs can be used to search single word or common Passwords); and
7. Common character sequences such as "123456" or same digit or letter such as "AAAA" or "11111".

There are also guidelines to unique passwords or passphrases that can be created by the following:

1. String several words together (these Passwords are also known as "passphrases"). An Example: IAmFast1.
2. Transform a regular word according to a specific method, such as changing a letter to a number reflecting its position in the word. An example: Applesauce becomes 1Pplesauce.
3. Combine punctuation or numbers with a regular word. An example: Texas = Tex1_2as.
4. Create acronyms from words in a song, a poem, or another known sequence of words. For example, the phrase "I want to eat strawberry ice cream in February", becomes: Iw2esiciF with the use of the number '2' for 'to'.
5. Combine a number of personal facts like birth dates and favorite colors "09Red14Blue56".

Users shall not display or store Passwords or passphrases in areas accessible to others, including but not limited to:

1. On a sticky note on your Workstation;
2. On a sticker on the bottom of your keyboard;
3. On the back of an employee badge; or
4. In an unlocked desk drawer

Regardless of the circumstance, Passwords and passphrases must never be shared or revealed to anyone (even family members) other than the authorized User. If Passwords are shared, any actions taken under the Password or passphrase shall be the responsibility of the authorized User. Passwords must be different for different accounts.

If Password or passphrase Security has been compromised, the Password or passphrase shall be changed immediately, and proper incident reporting procedures shall be followed. Withholding information related to Information

Security breaches or compromises can subject a User to disciplinary action, up to and including termination.

Procedures on User Terminations/ Monthly audits are implemented as follows:

- When a user is terminated in the Conifer HR system, a termination eID is generated automatically to remove user's access to Visual Cactus and assigned to VBC Support Desk.
- The eID is reviewed by the VBC Support Desk technician and the requested Visual Cactus account is disabled.
- In addition to the termination eIDs processing, the VBC IT team conducts monthly audits to ensure only the users active in the HR system have access to the application.
- Any access modification requires an eID submission even if the user currently has access to the application. (For example: If a user changes job title, a new eID request needs to be submitted to modify his/her Visual Cactus rights to reflect the new job title responsibilities).

Credentialing information will be released only under the following scenarios or situations:

- Requests made by Risk Management, corporate attorney, credentialing committee chairman etc. Reasonable efforts will be made to notify the impacted provider(s) prior to disclosure of information to attorney (s).
- Regulatory or Accreditation agencies – Access will require direct approval or supervision by the Credentialing Manager/Director to make sure no data is accessed without approval or authorization.
- Third parties (health plans, MCOs etc.) with whom delegate is contracted. Each provider must have a signed authorization and release form on file.

D. Credentialing Process Audit

Documentation for modifications that do not meet the established policy, the following will be implemented:

- For paper documents and files, the Credentialing Manager/Director will conduct periodic walk- throughs of the department to ensure that confidential/sensitive documents are being handled and stored properly during and after business hours. Examples of these are checking the fax machines if there are any documents laying around or on workstations, drawers are under lock and key etc.
- Incorporate review of data modifications/changes/updates to credentialing data (paper and electronic) into the file process. Assess and document findings for accuracy, appropriateness, and compliance with policies.

- Require credentialing staff to sign confidentiality forms and update on an annual basis.

An oversight of the credentialing modifications will include the following:

- Identify all modification to credentialing and recredentialing information that did not meet the organizations policies/procedures for modifications as in V. Element C above. A quarterly monitoring report will be generated to show compliance with the credentialing system policy which will include the following:
 1. Conduct a qualitative and quantitative analysis of all modifications that did not meet policies.
 2. Draw up actions to be taken to address any modifications that did not meet policy
 3. Implement quarterly monitoring and provide evidence of the review to the committee on an annual basis.
 4. Acting on all findings and implementing a quarterly monitoring process until it demonstrates improvement for one finding over three consecutive quarters.

The Credentialing Director/Senior Cred Specialist will conduct the above task. Attached are the tools (Attachment A & B) to be used in the implementation of the above task. These reports will be shared with committee.

Our database has a way of auditing information or tracking modifications through the audit log viewer in one of two ways: record level and field level. The audit log viewer allows users to view the changes made to records or fields for a designated time period. Field level will display the old and new values for the changes made to the field in the provider record. Each time a field is changed and saved, a new entry will be written into the audit log. On the other hand, record level once enabled will display when and who changed the record but will not track the old and new values for the field itself.

A semi-annual report will be generated listing the committee approved provider files that were processed, completed, and approved by the committee. From this report, we will complete an audit process by selecting a minimum of 10 initial credentialing and 10 recredentialing files. The credentialing lead/manager will review the selected files. An audit tool (based on NCQA/state standards) is used to determine whether or not the files are compliant with all required elements prior to credentialing committee review. The credentialing lead/manager will sign off on the completeness of the file. If the credentialing lead/manager finds any deficiencies in the file, it is returned to the credentialing specialist to further make the necessary follow up or complete whatever information needs to be added to the file. The credentialing lead/manager will maintain a score card of files

reviewed. The credentialing lead/manager will meet with the credentialing specialist if there are any trends or educational opportunities. The credentialing lead/manager will meet with the credentialing specialist if there are any trends or educational opportunities. All credentialing system audit reports will be presented to committee for approval.

VI. ENFORCEMENT

All employees whose responsibilities are affected by this policy are expected to be familiar with the basic procedures and responsibilities created by this policy. Failure to comply with this policy will be subject to appropriate performance management pursuant to all applicable policies and procedures, up to and including termination. Such performance management may also include modification of compensation, including any merit or discretionary compensation awards, as allowed by applicable law.

VII. REFERENCES

1. NCQA: CR 1 Element C 1
2. NCQA: CR 1 Element C 2
3. NCQA: CR 1 Element C 3
4. NCQA: CR 1 Element C 4
5. NCQA: CR 1 Element C 5

Revision History:

Version Date	Edited By	Reason for Change
01/01/21	R. Scott	Creation date
11/17/22	J. Moesche	Addition of NCQA CR 1 Elements 2-5