Credentialing System Controls Policy

Policy Number: COM.100

Version: 03

Contact: Mina Stier

Original Effective Date: 12.18.2019

Last Reviewed: 08.18.2022

Next Review/Approval Date: 08.31.2023

Credentialing System Controls Policy

POLICY: It is the Organization's policy to protect and control credentialing data and control access to the data. The Organization is committed to be the healthcare industry's preeminent provider of credentialing services. Part of that commitment is to maintain in absolute security and privacy all client and provider data. The Organization, as a credential verification organization (CVO), does not have access to health information or medical records. The Organization will follow industry and IT security and privacy best practices, while ensuring that its methods are consistent with HIPAA, HITECH, all applicable state and federal laws, and related CVO accreditation and regulatory organizations (e.g., CMS, NCQA, URAC).

SCOPE: This policy applies to all users of the credentialing operation systems; this includes primary and direct production and operations staff as well as support staff such as network engineers, software developers, quality personnel, management staff and other support roles. This policy will be reviewed annually, or upon significant changes that may occur in the organization environment, business circumstances, legal conditions, or technical environment to ensure their continuing adequacy and effectiveness.

PROCEDURES:

1. **CR 1.C.1. Receipt of Credentialing Information**
   A description of how credentialing information is received, stored, reviewed, tracked, and dated follows below:
   - **a.** Credentialing applications, supporting documents and verifications are received via (mail, email, fax, electronic application, online portal, internet web site or web crawler).
   - **b.** All documents are either dated electronically or date stamped when they are received and reviewed by Credentialing Staff.
   - **c.** File progress is tracked via an electronic credentialing checklist.
   - **d.** All files are stored in locked cabinets or file rooms and/or password protected database.
2. **CR 1.C.2. Tracking Modifications**
   A description of how the organization tracks modifications made to credentialing information follows below:
   - **a.** When a modification needs to be made to credentialing information, the Credentialing system will document the date and time the modification was made and who made the modification; the Credentialing specialist will include relevant explanations and reasons regarding the modifications. In CheckMedic this is documented in the MedPass Note data field; in Advantage and Synergy this is documented in the Request History field.
   - b. When data requires an update, such as when the element expires prior to delivery to the customer and requires a new verification, Verisys does not alter a previously

primary source verified record, the system prevents a modification; Verisys will create a new verification (based on current data). The original verification documentation is retained in the credential verification file. For modifications to primary source verified data, the Credentialing Specialist will document the change, contact method and/or name, and the Credentialing system will track the updates to include who made the update and the date and time it was made. The Credentialing Specialist data enters information regarding the update into the appropriate field (described above).

3. **Authorization to Modifications (CR 1.C.3)**

Authorization for modification will include the following requirements:

- **a.** Staff are assigned user roles based on areas of responsibility as defined in their job description.
- **b.** Each user role is assigned specific read/write system access as needed to perform their duties which may include modifying information; no user roles have rights to delete information.
- **c.** Verification information may be modified by Credentialing Verification Staff, 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 credentialing information include but are not limited to:

- To correct data entry errors
- Duplicate profiles
- Documents appended to incorrect provider profile
- Modifications to expired credentials

*The system does not allow for updates or modifications to verifications; a new verification record is required

***Inappropriate* modifications to credentialing information** include but are not limited to:

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

4. **Securing information (CR 1.C.4)**

A description of how credentialing information is secured from unauthorized modification is detailed in the Privacy, Security and Confidentiality Policy and Access Control Policy. The policies include, but are not limited to the following:

a. Hard copy data (any printed confidential/sensitive document or file) must be stored out of sight and not be accessible to anyone who does not have a business need to view the contents.
b. Credentialing staff shall secure all provider files and information when not in process and during non-work hours in locked cabinets in a restricted area that is only accessible to authorized staff.
c. Workstations are in physically secure areas.
d. Computer screens shall be positioned to prevent viewing by unauthorized individuals.
e. All password-based systems on workstations follow National Institute of Standards and Technology Guidelines; passwords are required to be strong; staff are discouraged from writing passwords down; user IDs and passwords are unique to each individual; passwords are required to be changed when requested or compromised; passwords are disabled or removed for employees leaving the organization; systems shall mask, suppress, or otherwise obscure the passwords so that unauthorized persons are not able to observe them.
f. Authorized users are prohibited from allowing others to access computer systems or restricted areas, including access by using their account, password, badge, or unique ID information.

Examples: When credentialing information may be released:

- Information will not be released without proper authorization
- Requests related to Compliance initiatives, Risk Management, Corporate Counsel concerns, or requests coming from the Credentialing Committee will be supported to respond to and/or to investigate credentialing or organizational concerns
- When applicable, reasonable efforts will be made to notify the impacted provider(s) prior to disclosure of information to attorney(s).
- Access to information by regulatory or accreditation agencies will require direct supervision by internal authorized personnel to ensure data is viewed in accordance with consent.
- Data access for third parties or organizations (health plans, MCOs, etc.) require an appropriate signed authorization/release form.

5. Compliance Monitoring (CR 1.C.5)

The credentialing process and controls will be audited by the Compliance Internal Audit department for compliance and will include the following assessments:

a. Entitlement Access: Annual review of job roles and current user access will be performed with the support of IT in order to ensure system access is appropriate for the role requirements.
b. Credentialing Data Accuracy: A minimum of an annual review of all modifications made to credentialing data in accordance with NCQA sample requirements as

applicable (that do not meet the organizations established policy) will be completed using system report functionality to confirm accuracy and appropriateness using the electronic system's audit trail function or change tracking reporting capability. The findings will be documented.

c. Credentialing Data Improvements: The organization will monitor (at least quarterly) the effectiveness of its action taken on all findings related to the credentialing data accuracy; the monitoring will continue until improvement has been demonstrated for one finding over at least three consecutive quarters.
d. Secure Documentation: For paper documents/files, periodic walk-throughs will be conducted to ensure confidential/sensitive documents are being handled and stored properly during and after business hours – i.e., in locked drawers/filing cabinets, not left on fax machines, etc.
e. Confidentiality Forms: The organization will require all credentialing staff and anyone who has access to credentialing information to sign an agreement to meet confidentiality requirements (where the confidentiality terms, contained in the organizations policies, will be reviewed annually, and updated as appropriate.)

6. Oversight of the Controls (CR 1.D)

The Credentialing System Controls oversight will include paper and electronic credentialing process; the oversight requires:

a. An annual monitoring report will be completed by the Compliance Officer, responsible for the monitoring activities and the oversight of the monitoring activities . At a minimum, the organization will produce an annual monitoring report to show compliance with the Credentialing System Controls policies, procedures and, if applicable Credentialing Delegation Agreement.

   The report will include:

   i. A review of all modifications that did not meet the organization's policies and procedures and/or delegation agreement.
   ii. A qualitative and quantitative analysis of all inappropriate modifications (where inappropriate modifications do not meet the organizations policies).
   iii. A documented account of the actions taken to address any inappropriate modifications that did not meet established policy, to include the implementation of a quarterly monitoring process of the actions taken.
   iv. An update on the quarterly monitoring and it will provide evidence of the review (of the quarterly monitoring).
   v. The person/role/title of the individual *or* name of the committee/body who performed the monitoring.
   vi. The person/role/title of the individual *or* name of the committee/body with oversight responsibility of the monitoring process, if different from who performs monitoring.

Oversight Reports are referred to as:

Credentialing System Controls Oversight Report – the report demonstrates the data oversight activities

Monitoring and Reporting of Inappropriate Modifications Report – the report provides data regarding if/when inappropriate modifications were identified.

7. **Performance Monitoring for Credentialing Delegation Agreements** (**CR 8.A.4)**
The credentialing delegation agreement will contain the Credentialing System Controls language ***OR*** the delegate will supply policies/procedures that include this language to meet the requirement.

8. **Annual monitoring of CR Systems for Credentialing Delegation Agreements (CR 8.C.5)**
The credentialing delegation oversight activities are required to include evidence of the Delegate's annual review of their Credentialing System Controls as outlined in NCQA CR 1 C factor 5. The requirements include submission of reports which identify any non-compliant modifications made to the Delegate's credentialing system/file.

    a. If the Delegate's system does not allow modifications, the evidence provided by the Delegate must provide the following:
        - A description of the functionality of the system that ensures compliance with established policy
        - Documentation or evidence of advanced system control capabilities that automatically record dates and prevent modifications that do not meet modification criteria
        - If the Delegate does not use a credentialing system that can identify all non-compliant modifications, auditing may be performed; the Delegate will be required to submit evidence and documentation

    Note: Automatic credit for this factor is made available to Delegates that are NCQA Accredited under 2022 (or later) standards for Health Plan Accreditation or CR Accreditation (not applicable to CVO Certification.)

9. **CR 8.C.6 Annual Actions taken by Delegated Entities**
Annual actions required by Delegated Entities, when the delegated entity identifies non-compliant modifications, in addition to the Delegated Entity completing quarterly oversight, Verisys will conduct quarterly oversight of the Delegated Entity until they can demonstrate improvement (of at least one finding) over three consecutive quarters. One action may be used to address more than one finding for the delegate.

    Note: Automatic credit for this factor is made available to Delegates that are NCQA Accredited under 2022 (or later) standards for Health Plan Accreditation or CR Accreditation (not applicable to CVO Certification.)

Exceptions:

The element is N/A if:

- Delegation arrangements have been in effect for less than 12 months, or

- The Delegate did not identify any modifications, or
- All identified modifications met the delegation agreement or met the delegate's policies and procedures for this requirement.

DEFINITIONS:

[Purposely left blank]

AFFILIATE PROCESSES/DOCUMENTS:

Privacy, Security, Confidentiality Policy

Access Control Policy

Records Retention Policy

Quality Management Program and Internal Quality Improvement Policy

Internal Audit of Completed Files Process & Procedure (PSV020)

REVISIONS LOG

Approval Date	Change Summary	Reason for Change
12.18.2019	Policy Created	Compliance
11.12.2020	Annual Review - Template Modification	Compliance
11.18.2021	Updated branding and template	Compliance
06.15.2022	Modified the procedure section of the document in order to meet NCQA's new and revised Credentialing System Control requirements	Compliance
08.18.2022	Updated to include additional detail and clarifications to procedures.	Compliance

REFERENCES

Source	Citation
NCQA Standards	CR: 1 Credentialing System Controls