PLAN OPERATIONS

Advantage Dental

From DentaQuest

*Policy and Procedure*

| | | | |
|---|---|---|---|
| Policy Name: | **Credentialing System Controls** | Policy ID: | **PLANCG-84** |
| Approved By: | Peer Review and Credentialing Committee | Last Revision Date: | 06/24/2025 |
| States: | Oregon | Last Review Date: | 06/25/2025 |
| Application: | Medicaid | Effective Date: | 06/26/2025 |

## PURPOSE

The DCO ensures that all data collected by the DCO credentialing department is entered correctly. The DCO ensures that the provider information/credentialing database is protected by password, limited to only those employees who require access and changes are limited to those with permission. The database is designed so that all changes made to the database are documented and recorded.

## POLICY

Provider information/credentialing information is documented accurately in the DCO database and protected from unauthorized change. The database controls include but are not limited to:

- Credentialing team staff will be trained on data entry with regular auditing for accuracy.
- Credentialing team staff will be trained on inappropriate modification of credentialing information.
- The database will be protected with passwords and change/view permissions appropriate to the user.
- The database will record changes made including date, time, and user.
- Database fields will be programmed to prevent duplication.

### Data Receipt

Information will be received in written form or electronically through web interface.

Information contained in the provider's record (to include the practitioner's application as well as attestation, primary source verifications, documentation of credentialing activities, reports, credentialing decisions, credentialing decision dates, credentialing checklist, verifier and reviewer signatures or initials, credentialing committee minutes, and documentation of clean file approval) are securely stored electronically in the Company's Credentialing system and available for review by only authorized staff.

### Access to Data and Provider Records

Credentialing management, leads and specialists have access to creating new provider records and making corrections to data entry errors.

Credentialing Leads and Specialists have access to create a new provider's record in the Credentialing System and enter all applicable credentialing information during the initial credentialing of the provider from their application and primary source verifications. Information obtained on an existing provider during a reapply or during recredentialing can be updated or edited according to the providers current application and primary source verifications. Modifications can be made to a provider's record to update verifications of expired credentials or to correct typographical errors. Credentialing specialists cannot delete credentialing system records.

Credentialing Management and System Administrators have access to making corrections to data entry errors; both changes and deletions, including typographic errors and duplicate records. These roles are responsible for oversight of credentialing information integrity functions, including auditing modifications.

Non-Credentialing Employees (Member Services and all other Plan Departments) have view only (non-editing) access to view certain provider information.

The Company's Credentialing system automatically tracks appropriate and inappropriate modifications including date and time made to a provider's record and stores historical information, which is available in the Activity Log. The Activity Log includes information on the field updated, the date and time and who updated the information. However, the Credentialing system does not track reasons for the change and is manually entered in the Notes section by the Credentialing staff.

Only authorized Credentialing Department staff as identified above, have modifying access to the credentialing system to enter/update provider information and to make modifications to the provider record, which include documenting primary source verifications and entering the credentialing and recredentialing date.

**Data Accuracy**

- Credentialing staff will be trained in how to enter data into the plan database.
- Annual audits will be conducted to verify data has been entered accurately.
- Annual audit will include 10 randomly selected files comparing original to entered data.
- Plan Reporting staff will conduct the annual audit.

**Monitoring of Data Accuracy and Inappropriate Modifications**
Plan Reporting and Compliance staff will conduct an annual audit of a random sampling to assess credentialing information for inappropriate documentation and updates.

- Annual audits will be conducted to verify data has been entered accurately.
- Annual audit will include 10 randomly selected files comparing original to entered data.
- The staff will select 10% or 10 (whichever is more) recredentialing and initial credentialing files. The samples will include only files with modifications.

The Audit Log report is saved and stored with the results from the audit. Any erroneous modifications that occurred will be researched and addressed with the specialist through additional training and documented. When erroneous modifications are found, quarterly monitoring will occur until findings show improvement for at least two (2) consecutive quarters. Any erroneous modifications will be corrected through this process. Any inappropriate modifications that occurred are researched and addressed with the specialist through additional training (as noted above) and documented via a corrective action plan. This plan will further explain any additional disciplinary action that needs to be taken with the specialist on a case-by-case basis, based on the severity of the modification and the frequency of the occurrence. An additional audit of the corrective action plan will occur within three (3) to six (6) months to review the effectiveness of the plan and ensure the inappropriate modifications were corrected. A qualitative analysis will be conducted if continued noncompliance is seen during the follow up audit. Audit results are reported quarterly to the Quality Improvement Committee for review. Any reports of fraud or misconduct will be reported to the NCQA.

Advantage requires all employees to adhere to its policies and procedures including those related to modifications to system and credentialing information.

**Database Protections**

- Users will be issued passwords for accessing the database. These passwords will be protected in the same manner as other enterprise issued passwords.
- Users will be assigned permissions within the database according to their position.

**Data Modification & Deletion**

- Credentialing Specialists and Above will be permitted to make modifications to data.
- Credentialing Managers and Above will be permitted to make deletions of data.
- Managers and above will have permission to request changes to fields names and formats.
- All users will have read only permission unless their position requires editing access.

**Database Change Documentation**

- The Database will record changes made to the data in the record history.
- The record history will show the time, date, and user who made the changes.
- The record history will include a revision history of each of the required fields.
- The change reason will be recorded in the record.

**Modification of Data**

When credentialing staff have a need to modify or delete data or documentation within the credentialing database, under the following circumstances authorized users may modify or delete:

- Update information during credentialing or re-credentialing
- Update information between credentialing cycles
- Update expired verifications during or between cycles
- Remove erroneous data or documentation

**Inappropriate Documentation and Updates**

The following documentation and updates to credential information are inappropriate:

- Falsifying credentialing dates (e.g., licensure date, credentialing decision date, staff verifier date, ongoing monitoring dates).
- o Creating documents without performing the required activities (e.g., photocopying a prior credential and updating information as a new credential).
- Fraudulently altering existing documents (e.g., credentialing minutes, clean-file reports, ongoing monitoring reports).
- Attributing verification or review to an individual who did not perform the activity.
- Updates to information by unauthorized individuals.

**Duplication Prevention**

Certain fields will be protected from containing duplicate data in the database. These fields include:

- State License Number
- Individual NPI

- Provider Social Security Number

**REFERENCES**
NCQA Credentialing Standards

***Revision History***

| Date: | Description |
|---|---|
| 1/15/2022 | Adoption And Approval |
| 02/20/2023 | Updates Made from CCO Findings |
| 04/26/2024 | Updates based on annual review. |
| 01/10/2025 | Updates based on annual review. |
| 06/24/2025 | Updated based on 2025 NCQA Credentialing Standards |