TEXAS TECH UNIVERSITY
HEALTH SCIENCES CENTER™
Paul L. Foster School *of* Medicine

Credentialing Office Policy and Procedure

Title: **PROTECTION OF THE CONFIDENTIALITY OF PROFESSIONAL STAFF RECORDS and CREDENTIALING SYSTEM CONTROLS**	Policy Number: **CO 1.2**
Regulation Reference: NCQA CR1.A, CR1EC.4, CR1.C Factors 1-5, CR1.D Factors 1-6	**Effective Date: 04-01-2012** **Last Annual Review Date: 11-04-2024** **Last Revision Date: 04-25-2025** (Revision History on last page)

Policy Statement:

It is the policy of Paul L. Foster School of Medicine (PLFSOM) to provide a safe, permanent repository for files of all Professional Staff members and applicants. Accordingly, disclosure of Professional Staff records shall only be permitted under the conditions set forth in this Policy and Procedure.

Procedure:

1. Location and Security Precaution

Each member of the Professional Staff has a credentials file on the credentialing electronic and/or paper file that is maintained in the Credentialing Office.

Paper files are stored in locked filing cabinets, in a locked room, only accessible by the Credentialing Office personnel. The building where this filing room is located can only be entered by personnel with a TTUHSC El Paso security badge. The file cabinets shall be locked except during such times Credentialing Office personnel is physically present.

The security of the credentialing database system has the following password-protective requirements:

- Password must not contain the user's name.
- Password must contain one English character (A through Z).
- Password must contain one Base 10 digit (0 through 9).
- Password must contain one non-alphanumeric character (e.g.,!, $, #).
- Password must be changed every 90 days
- Minimum unique passwords: 1

  and are also in accordance with the Texas Tech University Health Sciences Center El Paso (TTUHSCEP) Operating Policy and Procedure HSCEP OP: 56.01, HSCEP OP: 52.09 A. #2, #6, and HSCEP OP: 52.06, X and XI.

The Human Resources department provides a monthly employee termination report to the Director of the Credentialing Office, this report in turn is used to inactivate credentialing database access for all employees/personnel who have left TTUHSCEP.

The credentialing database system is accessed by approved Credentialing Office personnel. Each are assigned a unique username and password, with the above password protective requirements, staff is instructed to avoid writing down passwords.
The credentialing database system has an audit log capability, which allows the Director and Manager to be able to view all additions and modifications by user, which includes the date of when the action

was performed for each provider. When the Credentialing Office personnel needs to replace or update renewed data or documentation, they do not delete anything from the credentialing database system. Their function is to place all expired information/documentation as "Inactive", and then open an "Active" shell with the new or updated information/documentation.

2. Access by Personnel

Departmental Chairs or designees, PLFSOM Credentials Committee members, the Dean or designee and the Credentialing Office Staff shall have access to professional staff records only to the extent necessary to perform official functions.

a. Access by Personnel above or Professional Staff Functions

- All requests for Professional Staff Record by personnel shall be made to the Credentialing Office Director. A person permitted access under this policy shall be given a reasonable opportunity to inspect the records in question, under supervision and to make notes, but will not be allowed to remove them from the Credentialing Office or to make copies of them. Removal or copying shall only be allowed upon the permission of the Associate Dean Office of Clinical Affairs or his/her designated representative.

- Departmental Chairs or designees shall have access to all Professional Staff records pertaining to the activities of their respective departments.

- Professional Staff Committee members shall have access to the files in committee meetings of which they serve and to the credential and peer review files of practitioners whose competency or performance the committee is reviewing.

b. Access by Practitioners to their own Professional Staff Credentials Files

A practitioner may have supervised access to his/her own files during office hours (8 a.m. – 5 p.m.). The files may not be removed and may be read only in the presence of Credentials Office personnel. If any complaints are contained in the files, a written summary of complaints, deleting the names of the persons making the reports, will be placed in the files before it is made available to the individual practitioner. The Credentialing Office shall notify the individual when a written summary is required. If a written summary is required, it will take approximately two days before the files will be made available to the particular practitioner. This policy does not require PLFSOM to allow a practitioner to review references or recommendations or other information that is peer review protected. These will be removed from the file before review.

c. Access by other PSFSOM officials will only be permitted, if approved by the Office of General Counsel.

d. From a system level perspective, there are a number of controls in place:

- Data center firewall where rules determine what systems can access the server directly (Based on IT role).
- Antivirus software (Has EDR functionality and 24x7x365 monitoring by vendor).

- All logons/logoffs going to a SIEM (logs are kept for 1-year).
- Alerts from VMWare on any issues related to the server
- Rubrik allows us to monitor backup and restores for malicious activity.
- VMWare alerts of any abnormalities of the servers.
- DUO 2-factor authentication to access the server (Restricted by role to only specific IT positions).
- Servers are patched every 30-45 days.
- Change Management program to control changes.

From an application level perspective:

- Access is given to IT personnel based on role and not to all IT personnel.
- I.T. personnel only access the software based on helpdesk requests that are documented.

e. Vendors (i.e., custodial services) will have an executed business associate agreement in place to protect sensitive information and will be limited in physical access as appropriate to their job function.

3. Request by Persons or Organizations Outside of PLFSOM or its Professional Staff

   a. Routine Requests for Information: If a practitioner has not encountered disciplinary or peer review problems at PLFSOM, or been denied privileges at PLFSOM, then Credentialing personnel may respond to a request from another hospital or its medical staff. The request must be accompanied by the practitioner's signed consent to release information statement. Such routine requests must include notification that the practitioner is a member of or applicant to institutions Medical Staff. Disclosure of information shall be limited to the following: practitioner's status and category, dates affiliated with PLFSOM, and type of privileges granted.

   b. If a practitioner has been the subject of corrective action at PLFSOM, special care must be taken. All responses to inquiries regarding that practitioner shall be reviewed and approved by the Director of Credentialing Office who will seek consultation from Legal Counsel.

4. Request by Accrediting Organization, Governmental Surveyors or Managed Care Organizations

   Surveyors associated with accrediting, governmental or managed care organizations (TJC, NCQA, TDI, BCBS, Aetna, etc.) shall be entitled to inspect Professional Staff Records provided that the surveyor has:
   a. Specific statutory, regulatory, or other authority to review the requested materials, and
   b. Provided a written statement that the materials sought are directly relevant to the matter being investigated, and
   c. That the materials are the most direct and least intrusive means to carry out the survey or a pending investigation, bearing in mind that credentials/quality files regarding individual practitioners are strictly confidential.

   The surveyor may inspect Professional Staff Records via one of the following:
   1. On the premises in the presence of Credentialing Office personnel provided that no originals or copies are removed from the premises; and/or
   2. Secure desktop audit file submission via the following methods: secure email attachments, flash/thumb drive password protected, virtual access (auditor is allowed access to secure Texas

Tech system, or the health plan allows Credentialing Office personnel to share files in their secure system), or overnight mail service (FedEx, UPS)

5. Subpoenas

   All subpoenas of Professional Staff Records shall be referred to the PLFSOM Office of General Counsel Professional Liability Division.

6. Confidentiality Statement Form

   All Committee and staff members shall review and sign the confidentiality statement form annually.

7. Professional Staff Records Retention

   All professional staff records must be archived for 11 years, starting from termination/inactivation date from the professional staff.

8. Policy CO 1.2 will be reviewed with any new hiring staff or members of the Credentials Committee, within 90 days of hire. Policy will be reviewed with all staff and committee members on an annual basis as part of employee training / annual review of policies.

9. Integrity of Credentialing Files

   Per policy CO 1.3 – Right of Notification and Correction of Information, CO 1.5 – Initial Application / Appointment to Professional Staff, and CO 1.6 – Reappointment / Re-credentialing Application to Professional Staff are received via mail, email, or fax. Staff will date stamp and initial all received application forms, supporting documentation, primary source verifications, and any corrections by the practitioner or primary source verification. All documents received are reviewed by the Credentialing Office staff and tracked via the provider checklist and electronic database.

   We protect all credentialing and recredentialing information obtained to include:

   - The practitioner application and attestation
   - Credentialing documents received from the source or agent
   - Documentation of credentialing activities such as verification dates, report dates (e.g., sanctions, complaints, identified adverse events)
   - Credentialing decisions
   - Credentialing decision dates
   - Signature or initials of the verifier or reviewer
   - Credentialing Committee minutes
   - Documentation of clean file approval
   - Credentialing checklist

   Documents received are never modified by the Credentialing Office. Updates are only made to the database system when corrected and/or modified information is received, by either fax, email or mail, from the provider or the actual primary source verification/verifier, in order to maintain accuracy of

provider's data. The Credentialing Office shall document the reason for modification, as stated below. All credentialing forms will be placed in the provider's permanent paper and/or electronic credentialing file. All documents received in the credentialing process shall then be taken through the Credentialing approval process.

When corrected and/or modified information is received, the Credentialing Office staff must include in the provider's permanent paper and/or electronic credentialing file:

1. Why the credentialing information was corrected/modified;
2. When the credentialing information was corrected/modified;
3. How the credentialing information was modified, or area where the modification was made;
4. And the staff who modified the credentialing information, with their initials and date-stamp.

Credentialing Office staff authorized to modify or correct information, where determined appropriate are the Director, Manager, and Credentialing Specialists in the office.

At the start of each year annual training will be held for the credentialing staff which will include:

- Training on inappropriate documentation and updates to credentialing information
- Training to inform staff on audits of staff documentation updates in credentialing files
- Training on the process for documenting and reporting inappropriate documentation and updates to staff individual(s) when identified, and health plan when it identifies fraud and misconduct.
- The consequences for inappropriate documentation and updates

Credentialing Director or Manager will review and monitor the credentialing staff work at the time of initial credentialing and at the time of each subsequent re-credentialing, the provider profile will be signed and dated by the reviewer. Additionally, external audits feedback will be reviewed annually.

Annually at the end of each year, the Credentialing Director or Manager will review the required amount of provider files in the credentialing database system (Minimum of 10 initial appointments and 10 re-credentialing appointments). The files reviewed and their results, will be recorded in the Annual CR Information Integrity Assessment Reporting Tool. . The review will focus on the integrity of the credentialing process and files, to make certain no changes, deletions, or modifications were made that were not consistent with the credentialing process or as a result from primary source verifications. Any identified deficiencies, will be addressed accordingly and by following the institutions Texas Tech University System Regulation 07.07 – Employee Conduct, Coaching, Corrective Action, and Termination policy process and reported to the Credentials Committee and Health Plans.

If deficiencies such as falsifying credentialing dates, creating documents without performing the required activities, fraudulently altering existing documents, attributing verification or review to an individual who did not perform the activity, updates to information by unauthorized individuals are identified, the Credentialing Director or Manager will take appropriate action to address the deficiency and ensure that employee must adhere to the Employee Conduct, Coaching, Corrective Action, and Termination policy process imposed to them, as applicable. A quarterly monitoring process must be in place in order to assess the effectiveness of the action taken, until such time that it demonstrates improvement or final resolution but for at least three consecutive quarters.

Electronic documents are stored in the departments password protected credentialing database, or individual TTUHSC El Paso Credentialing Office personnel computer systems, as mentioned in #1, and only accessible by the Credentialing Office or any approved TTUHSCEP personnel, and who will comply with TTUHSCEP Operating Policy and Procedure HSCEP OP: 56.01, HSCEP OP: 52.09 A. #2, #6, and HSCEP OP: 52.06, X and XI.

Policy Number:	**CO 1.2**		Version Number: **1.0**
Signatory approval on file by:	**Approved:**	Adam H. Adler, M.D., Chair, TTUHSCEP PLFSOM Credentials Committee	

Revision History		
	Credentials Committee	Dean Approval
Effective Date:	04-01-12	
Annual Review Date:	03-25-19, 01-30-20, 02-23-21, 01-26-22, 09-27-23, 10-30-24	03-26-19, 01-30-20, 02-23-21, 01-28-22, 09-29-23, 11-04-24
Revision Date:	03-31-16, 02-27-18, 05-23-18, 09-25-18, 10-29-19, 02-25-20, 02-23-21, 07-13-21, 11-16-21, 03-23-22, 07-26-22, 01-24-24, 05-22-24, 04/21/2025	03-31-16, 02-28-18, 05-24-18, 09-27-18, 10-31-19, 02-27-20, 02-23-21, 07-15-21, 11-17-21, 03-25-22, 07-28-22, 01-29-24, 05-24-24, 04/25/2025