IDENT	UVMHN C&E 101
Type of Document:	Policy
Type of Policy:	Department
Applicability:	All
Sponsor's Dept:	Credentialing & Enrollment
Title of Owner:	Director
Title of Approving Official:	UVMHN C&E Medical Director
Date Released (Published):	Amended and restated, 02/21/2025
Next Review Date:	1 year from last Date Approved

SUBJECT: Credentialing System Controls, Access, Confidentiality & Credentialing Information Integrity.

PURPOSE: To ensure departmental process and expectations are in line with organizational policies and NCQA Standards surrounding confidentiality, protection of information, physical access to credentialing information, personnel management, information security, and modification of credentialing information.

POLICY STATEMENT: UVMHN Credentialing & Enrollment (UVMHN C&E) in collaboration with the UVM Health Network (UVMHN) Information Security Department and C&E software vendor shall be responsible for ensuring that reasonable safeguards have been established to protect the confidentiality and integrity of all records, discussions and documentation related to credentialing activities performed by UVMHN C&E pursuant to primary source verification and ongoing monitoring.

PROCEDURE:

LOCATION, SECURITY, AND ACCESS TO CREDENTIAL FILES

1. Practitioner credentialing information shall be maintained under the care and custody of the UVMHN C&E staff. As applicable to paper records, the offices and file cabinets where credentialing information is stored shall be kept locked, except when an authorized representative supervises access. Electronic records shall be protected by unique user ID & passwords and read/write controls and stored in the UVMHN Credentialing Software system.

   1.1 Credentialing Information includes but is not limited to:
   - 1.1.1 The practitioner application and attestation
   - 1.1.2 Credentialing documents including those provided by the applicant/agent and acquired for PSV
   - 1.1.3 Documentation of credentialing activities including -
     - 1.1.3.1 Verification dates
     - 1.1.3.2 Report dates (sanctions, complaints, and identified adverse events)
     - 1.1.3.3 Credentialing decisions
     - 1.1.3.4 Signature or initials of the verifier or reviewer
   - 1.1.4 Credentialing Committee minutes
   - 1.1.5 Documentation of clean file approval, if applicable
   - 1.1.6 Credentialing checklist, if used.

   1.2 See Policy C&E 10 Credentialing Recredentialing Processes for details on how primary source information is received and dated.
2. Authorized access is granted to the staff and leadership of UVMHN C&E Department, as well as the UVMHN C&E Medical Director, the UVMHN C&E Credentials Committee, and the UVMHN C&E Board of Directors as needed to discharge their lawful obligations and responsibilities.
3. In collaboration with and as subject to C&E's existing contract with software vendor, all Credentialing & Enrollment computer security requirements for electronic information systems belong to UVMMC/UVMHN and are subject to the responsibilities and standards for the

UVMMC/UVMHN Information Security Program which ensures adequate security measures are in place to protect computer resources (i.e., the information stored in or processed by computers, the equipment and the software).

4. Credentialing & Enrollment staff shall be subject to and shall maintain compliance with the entire UVMHN Policy UVMHN_INFO4 *Information Security Program Policy,* UVMHN_INFO5 Information Security User Policy, *INFOPOL3 Enterprise Data Backup and Retention Policy & INFOPOL1 Computer Room and Network Access Policy for the Data Centers and Network Closets* including, but not limited to:

4.1 Roles & Responsibilities

4.1.1 System(s) Users – responsibilities of all users of UVMMC/UVMHN resources include, but are not limited to:

4.1.1.1 Users are not allowed to permit others to access UVMMC/UVMHN computer systems with their account, password, badge and OneSign PIN. Users are responsible for activity conducted under their Account ID.

4.1.2 Directors & Supervisors – notification to Application Access Team of Information Security is required whenever:

4.1.2.1 Any individual over whom you may have oversight terminates or otherwise has a change in their computer/network access needs.

4.1.2.1.1.1 Leadership also has the following responsibilities in ensuring compliance with the information Security Program.

4.1.2.1.1.1.1 Requesting new accounts or changes to access.

4.1.2.1.1.2 Software Vendor

4.1.2.1.1.2.1 Must maintain compliance with its contract, all related documents or amendments to the contract with the University of Vermont Health Network.

4.2 Access Controls

4.2.1 User IDs (System Accounts) -User IDs for network and access to various systems are issued and maintained by the Application Access Team. Those not maintained by the Application Access Team have a designated System Security Administrator which is documented in the System Security Administration Procedure for that system.

4.2.1.1 User IDs (accounts) are assigned to new users who require computer access at the beginning of their employment or contract with UVMMC/UVMHN and may also be assigned subsequently when the individual takes on additional duties and/or responsibilities, or when reassigned/transferred within UVMMC/UVMHN.

4.2.1.1.1 When new accounts are made active, users are informed of their responsibilities regarding confidentiality of electronic systems and data during New Employee Orientation where they also get their m-number and password from an Information Security representative. New employees sign a UVMMC/UVMHN Employee Confidentiality Statement at orientation which covers all paper and electronic records.

4.2.1.1.1.1 Staff has access to change their password if requested or if passwords are compromised.

4.2.1.1.2 User IDs for UVMMC/UVMHN support systems and the user's access levels are granted based on a business need as determined by the job description or function being performed (role-based access).

4.2.1.1.3 User IDs (accounts) are deactivated when the need for access no longer exists. Examples include, but are not limited to, termination of employment, job transfer, or termination of a contract. It is the responsibility of the UVMMC/UVMHN Management to notify IS Service Center immediately when a user ID should be deactivated.

4.2.1.2 Closing User Accounts - Closing of user accounts is handled by the Application Access team, the IS Service Center, and IS Operations. There are several different circumstances that determine the procedures and notification times involved. In all cases the employee's supervisor is responsible to ensure that all confidential and sensitive computer media is returned to UVMMC/UVMHN.

4.2.1.3 Time Outs - All computers are subject to an automatic "time-out" of inactive user accounts.

4.2.1.4 Passwords - All password-based access control systems on workstations must mask, suppress, or otherwise obscure the passwords so that unauthorized persons are not able to observe them.

4.2.1.4.1 Workstations will be located in physically secure areas and their display screens must be positioned so as to prevent unauthorized viewing by visitors.

4.2.1.4.2 Passwords must be a minimum length of 8 characters; use a 3 out of 4 password complexity (Upper, Lower, Numbers, Symbols); are required to change every ninety days; may not use any of the last 10 passwords.

4.3 Electric Communications

4.3.1 E-Mail

4.3.1.1 The e-mail systems provided by UVMMC/UVMHN are owned by UVMMC/UVMHN and are provided for conducting official business. All data on these systems, including e-mail, are the property of UVMMC/UVMHN. Employees should not have an expectation that e-mail is private. Contents can be monitored, and review of employee e-mail may occur when a business situation so warrants.

4.3.1.2 All email addressed to users outside of the UVMMC/UVMHN email domain (uvmhealth.org) will contain the following notice:

Confidentiality Notice: This message and any attachments may contain information that is confidential, privileged and/or protected from disclosure under state and federal laws. If you received this message in error or through inappropriate means, please reply to this message to notify the Sender that the message was received by you in error, and then permanently delete this message from all storage media, without forwarding or retaining a copy.

4.3.2 Instant Messaging - Instant Messaging services are available using Skype for Business or Microsoft Teams. No other instant messaging software/system is

allowed. Instant Messaging may not be used to send CI or other sensitive information.

4.3.3 Security of UVMMC/UVMHN e-mail

4.3.3.1 Sending Confidential Information (CI) outside of the UVMMC/UVMHN Health Care Network is strictly prohibited unless the information has been encrypted.

4.3.3.2 Requirements for securing email - The following should be used when sending CI to other recipients:

4.3.3.2.1 Verify the email address you are sending to is correct.

4.3.3.2.2 Send the minimum amount of PHI / CI required pursuant to UVMMC/UVMHN privacy policies.

4.3.3.2.3 Encrypt the email by hitting the “encrypt” button or typing SECURE# into the subject bar.

4.3.3.2.4 Verify email was received.

4.3.3.3 Information given to others by UVMMC/UVMHN users must be protected in accordance with the UVMMC/UVMHN Confidentiality Policies (Appendix A).

4.4 Use of the Internet

4.4.1 Internet Resources – All employees are encouraged to use Internet services in support of their work. While doing so, all employees are expected to conduct their use of these services with the same integrity as in face-to-face or telephonic business operations. Additionally, users must be aware that UVMMC/UVMHN monitors access to these services to protect the liability of the organization and to ensure policy compliance. Access to the Internet from home or elsewhere via UVMMC/UVMHN provided connections or computers must adhere to all of the same policies that apply to use from within UVMMC/UVMHN facilities.

4.5 Confidentiality

4.5.1 UVMHN Confidentiality Policy

4.5.1.1 UVMMC/UVMHN has several policies that govern the confidentiality of patient and/or business information. It is the expectation of UVMHN C&E leadership that all employees will be familiar with and remain in compliance with all policies as related to confidentiality.

4.5.2 Control and Storage of Confidential and Sensitive Data

4.5.2.1 Workstations may not be used as a repository to store electronic confidential information (CI) on the local hard drive (most often the "C:" drive). Network drives should be used for the storage of confidential and sensitive information.

4.5.2.2 UVMMC/UVMHN confidential data stored on portable storage media (e.g., diskettes, tapes, CD-ROMs, flash/thumb drives) must be secured at all times when not in use and stored on an approved encrypted device if the data contains CI. Approved storage includes inside a locked desk drawer, a locked file cabinet, a safe/security container, or a similar lockable device that would provide like security.

4.5.2.3 Transferring confidential or sensitive information to unencrypted or personally owned portable devices is not authorized with the exception of syncing UVMMC/UVMHN email to their personal mobile devices. If

UVMMC/UVMHN data is stored on a personal mobile device, Information Security reserves the right to remotely wipe the device if it is reported lost or stolen or if the user's employment is terminated.

4.5.2.4 Data in Hardcopy - Any printed UVMMC/UVMHN confidential/sensitive data must be stored out of sight and not be accessible to anyone who does not have a business need to view the contents.

4.5.2.5 All laptops and other portable devices purchased with UVMMC/UVMHN funds or placed on the UVMMC/UVMHN network must be encrypted.

4.5.3 Disposal of Electronic Confidential and Sensitive Data - Confidential data stored on computers and portable storage media (tape cartridges, diskettes, CD-ROMs, etc.) must be removed entirely before reuse, disposing of, or transferring out of UVMHN C&E's control. The physical disk drives must be placed in a locked bin which is picked up by a third party for destruction.

4.5.4 Transmission of Confidential and Sensitive Data

4.5.4.1 E-mail - see Electronic Communications above.

4.5.4.2 Internet - Confidential data should not be transmitted over the Internet unless business operations require its use. Confidential data must be encrypted when sent over the Internet.

4.5.4.3 Facsimiles (Fax) - When using a fax machine, the sender must ensure the phone number is correct. Faxes that will be used to receive confidential information must be located away from the general public, in areas where only those with a need for the information can access the machine. Cover sheets should be used whenever faxing confidential or sensitive information.

4.5.5 Lost or Stolen Devices - If a device containing confidential or other sensitive information is suspected to be lost or stolen, it must be reported to the Service Center immediately.

4.6 Computer Security Awareness and Education –

4.6.1 The objective is to ensure that all employees are aware of their role in protecting information services resources and the electronic data stored within them, and to improve information security skills and awareness of possible security problems or risks.

4.6.2 New Employee Orientation – All employees will participate in a block of instruction which will provide an overview of information services security policies and provide tips on good computer security practices.

4.6.3 Mandatory Refresher Training – All users are required to participate in an annual online training regarding information security.

4.7 Exceptions to Policy – Exceptions to this policy will not be granted if the integrity and security of applications and/or the network will be placed at increased risk.

ACCESS TO CREDENTIALING & ENROLLMENT DEPARTMENT

1. Access to Credentialing & Enrollment Department

1.1. The Credentialing & Enrollment Department is secured by a limited access entryway. Each authorized party is assigned a badge number for individualized access which will be removed from the prox card system when the individual no longer requires access to the Credentialing & Enrollment Department.

1.2. The Credentialing & Enrollment staff offices, including computer hardware are secured by locked and user specific keycard access doors.

1.3. The Credentialing & Enrollment staff cubicle file cabinets are secured by lock mechanisms.
1.4. The Credentialing & Enrollment Server is secured by locked and user specific keycard access doors.
1.5. Credentialing & Enrollment staff shall access only those practitioner files that are within their purview.
1.6. Credentialing & Enrollment staff shall secure all practitioner files and information when not in process and during non-work hours.

2. Access by individuals performing official functions.
   2.1. Upon the request of the Director of Risk Management, consultants or attorneys engaged by The University of Vermont Health Network may be provided with relevant records that are necessary to enable them to perform their functions. Reasonable efforts will be made to notify the practitioner prior to the disclosure of any information to consultants or attorneys.
   2.2. Representatives of regulatory or accreditation agencies may have access to records that may be necessary to enable them to perform their functions.
   2.3. Authorized third parties and/or representatives from organizations for whom UVMHN C&E performs delegated credentialing services may have access to records pertaining to their applicants or participating providers, provided that each applicant or participating provider has completed a satisfactory authorization and release form.
   2.4. Visitors, such as auditing representatives of Payors, must be escorted at all times by at least one Credentialing & Enrollment employee to consider them to be under escort.
3. Access by practitioners shall be granted for access to his or her own credentials file, subject to the following procedure:
   3.1. Requests to review a file shall be made to the Director, Credentialing & Enrollment, or designee. The review will take place in the Credentialing & Enrollment office during normal office hours.
   3.2. The practitioner shall have access to contents of file components under supervision of Credentialing & Enrollment staffing in accordance with the UVMHN ***Policy C&E 8*** (Practitioner Confidentiality).

ACCESS TO CREDENTIALING SOFTWARE SYSTEM

1. Access to Software System
   1.1. The software system is secured by user ID and password utilizing single sign on methodology. Each authorized party is granted access through direct authorization by the Credentialing & Enrollment Department Director.
   1.2. Application Analyst for software system has responsibility to maintain a master document with all users to the system which includes their user role and purpose for access, including if user role permits read only, write, or delete privileges. All users and their respective user roles are assessed at least bi-annually with the Director of Credentialing & Enrollment for appropriateness of ongoing security access.
2. Access by Credentialing & Enrollment staff
   2.1. Credentialing & Enrollment staff are assigned user roles based on areas of responsibility as delineated in specific job descriptions for their role. Each user role is assigned specific read/write access on a need-to-know basis for the purposes of performing their duties. Credentialing & Enrollment staff are expected to follow *UVMHN_INFO5 Information Security User Policy* for securing their workstation when not present.
3. Access by individuals performing other duties to which access to data is deemed necessary to perform their duties.
   3.1. Organizational leaders of non-Credentialing & Enrollment staff must submit a detailed request for provision of access to credentialing software system directly to the Credentialing & Enrollment Department Director. If request is approved, access will be granted following the same process delineated above, including assignment to a specific user group with individual read/write access and limited to only the minimum information needed to perform the duties of the non-Credentialing & Enrollment staff members.

3.2. Representatives of regulatory or accreditation agencies may have access to records that may be necessary to enable them to perform their functions. This access will require direct supervision by a Director, Manager or Supervisor within the Credentialing & Enrollment Department to ensure that no data is accessed without authorization.

3.3. Authorized third parties and/or representatives from organizations for whom UVMHN C&E performs delegated credentialing services may have access to records pertaining to their applicants or participating providers, provided that each applicant or participating provider has completed a satisfactory authorization and release form, the individual granted access completes the Credentialing & Enrollment Confidentiality and Agreement, and agrees to abide by all aspects of this policy and the *UVMHN_INFO5 Information Security User Policy* as deemed applicable.

3.4. Visitors, such as auditing representatives of Payors, will require direct supervision by a Director, Manager or Supervisor within the Credentialing & Enrollment Department at all times to ensure that no data is accessed without authorization.

4. Access Audit

4.1. Information System Audits

4.1.1. Credentialing & Enrollment staff shall be subject to and shall maintain compliance with all UVMHN Information Services Policies, as applicable.

4.2. Routine C&E Department System Audits

4.2.1. Department Leadership will conduct audits regularly (paper or electronic), at least every 2 months, of completed initial and re-credentialing files, specifically reviewing for modification & data integrity of provider data from its initial or subsequently verified state. The audits will be focused on identifying and assessing risk to ensure that UVMMC/UVMHN Information Systems and UVMHN Credentialing & Enrollment policies and procedures are followed.

4.2.2. Audit Methodology

4.2.2.1. Initial Credential Records

4.2.2.1.1. To be performed for each specialist who has completed initial credential records with the previous credentialing cycle.

4.2.2.1.2. Audits will be performed on a random selection of records as indicated.

4.2.2.1.3. A minimum of 3 provider records per specialist, or a minimum 10 total provider records depending on the number of specialists that will be reviewed during each audit cycle.

4.2.2.1.4. All data forms per provider record will be reviewed. Forms audited include Demographics, License, Group Address Information, Specialty/Boards, Insurance, Education and Work History. As applicable to provider type Alternate Providers form may also be reviewed.

4.2.2.1.5. Evidence of audit, including supporting documentation will be maintained for each specialist. The Bi-Monthly, Year Review and Semi-Annual & Annual Summary audit findings will be presented to the UVMHN Payor Network Credentials Committee as part of the internal department quality improvement reports.

4.2.2.2. Re-credential Records

4.2.2.2.1. To be performed for each specialist completed re-credential records within the previous re-credentialing cycle.

4.2.2.2.2. Audits will be performed on a random selection of records as indicated.

4.2.2.2.3. A minimum of 5 provider records per specialist, or a minimum 10 total provider records depending on the number of specialists that will be reviewed during each audit cycle.

4.2.2.2.4. All data forms per provider record will be reviewed. Forms audited include Demographics, License, Group Address Information, Specialty/Boards, and Insurance. As applicable to provider type Alternate Providers form may also be reviewed.

MODIFICATIONS TO CREDENTIALING INFORMATION

1. Authorization to Modify
   - 1.1. Each user role is granted access to modify data based on job responsibilities.
     - 1.1.1. Each user role may include permission to create new data records, change existing records, or delete information.
     - 1.1.2. Each role is documented in a shared location by user group title, individual users, entity assignments and read/write/delete permissions; these roles and document is managed and maintained by the System Administrator in collaboration with the Business Administrator for the software system.
   - 1.2. Deletion of any data within the provider record requires authorization by a member of the department leadership team or Data Integrity & Training Specialist
2. Circumstances for Modification
   - 2.1. Addition of a New Data Record
     - 2.1.1. When information is provided by an applicant and can be primary source verified by a credentialing specialist or other member of the credentialing team.
     - 2.1.2. When information is provided by an application that does not require primary source verification such as certain demographic information and alternate practice location information.
   - 2.2. Change to Existing Data Record
     - 2.2.1. When primary source verification indicates that previously verified information has been updated or revised.
     - 2.2.2. When a primary source reports an update to information, they previously provided that initially contained an error in the verified information.
     - 2.2.3. When previously entered, information is determined to have been entered in error.
     - 2.2.4. When an applicant reports an update to previously entered, non-verified (does not require primary source verification) information such as certain demographic and alternate practice location information.
     - 2.2.5. When previously verified information, such as a current license, is verified at a future credentialing instance as no longer active, the data record can be inactivated but will not be deleted.
   - 2.3. Deletion of an Existing Data Record
     - 2.3.1. When primary source verification indicates that information reported by the applicant was incomplete, inaccurate, or was part of a separate data record and the creation of this record would represent false, missing, or incomplete information.
     - 2.3.2. When a primary source reports an update to information, they previously provided that initially contained an error in the verified information or legal action requires that they modify the information previously provided such that the data recorded is no longer appropriate to this record. Example – NPDB report returned indicating that previously provided information must be stricken from the provider's credentialing record.
     - 2.3.3. When an applicant reports that previously provided information that does not require primary source verification should be removed from the application due to an error in the data provided.
     - 2.3.4. When a member of the credentialing team enters data to the provider record in error.
   - 2.4. Tracking Modifications
     - 2.4.1. Software system provides an automated mechanism to track modifications to provider data which includes when the information was modified (including date and time), how it was modified and who made the modification via an audit log report.
       - 2.4.1.1. C&E Leadership reviews software audit report on a regular basis through its established record audit procedures outlined above.
       - 2.4.1.2. C&E Leadership reviews software audit report on an as needed basis for cause when there is reason to believe that information may have been modified in error.
       - 2.4.1.3. C&E Leadership performs periodic random audits when reviewing provider records for modification of data.

2.4.2. Modification of data record is validated by one of the following mechanisms, which must be present in the provider's record to support and track the reason why a change was made:
2.4.2.1. Primary Source Verification
2.4.2.2. Secondary Source Verification
2.4.2.3. CAQH
2.4.2.4. UVMHN Application
2.4.2.5. Other Documentation provided by Applicant or Representative
2.4.2.6. C&E Add/Change/Term Form

INAPPROPRIATE DOCUMENTATION AND UPDATES

1. The modifications to documentation and information listed below are deemed inappropriate under this policy to uphold the integrity, accuracy, and reliability of all records.
   1.1. Falsifying credentialing dates (e.g., licensure date, credentialing decision date, staff verifier date, ongoing monitoring dates).
   1.2. Creating documents without performing the required activities (e.g., photocopying a prior credential and updating information as new credential).
   1.3. Fraudulently altering existing documents (e.g., credentialing minutes, clean-file reports, ongoing monitoring reports).
   1.4. Attributing verification or review to an individual who did not perform the activity.
   1.5. Updates to information by unauthorized individuals.

MONITORING OF COMPLIANCE

1. Supervisor of Payor Services audits all new and recredentialed provider files for compliance with all data points including but not limited to established primary source verification processes (how data it is received, dated and stored) monthly.
2. Supervisor of Payor Services performs (at a minimum yearly) software system audits of modifications to provider data, including documents from its initial verification as outlined in section 4 of the UVMHN C&E 101 – Credentialing System Controls, Access & Credentialing Information Integrity policy.
3. The Application Analyst for software system and the Director of Credentialing & Enrollment assess all user roles and individual users assigned to each role at least every 3 months for appropriateness of ongoing security access. See section 1 of the UVMHN C&E – Credentialing System Controls, Access & Credentialing Information Integrity Policy.
4. The UVMHN IT Security team along with the UVMHN Security team are responsible for building security related to the protection of electronic systems which hold credentials information.

MONITORING SYSTEM ACCESS

1. The credentialing software program maintains historical change data tracking to identify who has accessed the system, when and what actions were taken. The system provides reports on demand and will be run at a minimum yearly. The Credentialing & Enrollment Director or Supervisor generates and reviews activity reports.

CORRECTIVE ACTION

1. The following corrective action will take place for inappropriate modification of data: The UVM Medical Center reserves the right to exercise corrective action it deems appropriate given the circumstance.
   1.1. Credentialing Specialist will be required to review Policy 101
   1.2. The Supervisor or Director will go over the modification(s) of data with the specialist. Upon review of the details the Supervisor or Director will make a determination if the modification(s) were completed in error or due to malintent.
      1.2.1. If the determination is made that the modification(s) were completed in error:
         1.2.1.1. The Credentialing Specialist will be provided with education and training.

1.2.1.2. The Supervisor or Director will run Monthly reports for 3 consecutive months to monitor/analysis for inappropriate modifications, draw conclusion about the action(s) effectiveness and will discuss with specialist as necessary.

1.2.1.2.1. If additional inappropriate modifications are still being made after 3 consecutive months, Supervisor or Director will take corrective action, up to and including termination, in accordance with the UVMHN Corrective Action Policy.

1.2.2. If the determination is made that the modification(s) were intentional:

1.2.2.1. This activity will be addressed by corrective action, up to and including termination, in accordance with the UVMHN Corrective Action Policy.

2. In cases of a breach of confidentiality or if there is reason to believe that information has been shared in violation of this policy. The Director or Supervisor of Credentialing & Enrollment will request the relevant report(s). Appropriate actions will then be taken, up to and including termination, in accordance with the UVMHN Corrective Action policy.
3. Identified inappropriate access will be addressed by corrective action, up to and including termination, in accordance with the UVMHN Corrective Action policy.

DOCUMENTING AND REPORTING INTERGRITY ISSUES

1. UVMHN C&E utilizes the Annual CR Information Integrity Assessment Reporting Tool (sample attached), for documenting, analyzing and reporting yearly audit.
   1.1. The Audit and analysis report includes:
      1.1.1. The report date
      1.1.2. The title of individuals who conducted the audit
      1.1.3. The 5% or 50 Files auditing methodology
         1.1.3.1. Auditing period
         1.1.3.2. File audit universe size
         1.1.3.3. Audit sample size
      1.1.4. The audit log (Annual CR Information Integrity Assessment Reporting Tool)
         1.1.4.1. File identifier (individual practitioner)
         1.1.4.2. Type of credentialing information audited
      1.1.5. Findings for each file
         1.1.5.1. A rational for inappropriate documentation and updates
      1.1.6. The number or percentage and total inappropriate documentations and updates by type or credentialing information
2. Annual CR Information Integrity Assessment Reporting tool will be shared with UVMHN C&E's end user, Director of Credentialing and Enrollment and the UVMHN Credentials Committee.
3. Information on CR Information Integrity Assessment Reporting tool will be shared with NCQA (when identified as fraud or misconduct)
   3.1. When reporting to NCQA, Section 5 (Reporting Hotline for Fraud and Misconduct, Notifying NCQA or Reportable Events) located in the NCQA CRPN (Standards and Guidelines for Accreditation and Certification in Credentialing and Provider Network) will be reviewed and followed.

Important Note – UVM Health Network Credentialing & Enrollment Staff are subject to compliance with UVMMC/UVMHN policies, as applicable. UVMHN C&E staff are employees of UVM Medical Center. The C&E operates as a department of UVM Health Network. UVMHN C&E's software contract is held by the UVMHN.

EMPLOYEE RESPONSIBILITES

1. Orientation - Credentialing & Enrollment staff shall be subject to and required to attend the UVMMC/UVMHN New Employee Orientation. In addition to this, all staff will receive training including, but not limited completion of an initial departmental orientation upon joining Credentialing & Enrollment. As part of a new employee's initial briefing at their department level, directors, managers and supervisors should address items as delineated in the *C&E Orientation Checklist for New Employees* including but not limited to where the employee can dispose of

confidential material, to which they report computer security incidents, office procedures related to computer security, etc.

2. Confidentiality - Credentialing & Enrollment staff are required to be familiar and in compliance with the UVMHN Comprehensive Confidentiality Policy. In addition to this all C&E employees will complete and sign initially upon hire and annually thereafter a *Confidentiality and Conflict of Interest Agreement* which includes a Non-Discrimination Agreement statement.
3. Identification – As per the following UVMHN policy all employees will wear Identification Badges as provided.
4. Assess & Use of Provider Data - It is the expectation that all staff will only access provider records and will utilize confidential information on a "need-to-know" basis.
5. Training – UVMHN annually trains Payor credentialing and re-credentialing Specialist and additional staff as applicable on inappropriate documentation and updates to credentialing information starting prior to 07/01/2025 and the beginning of each year thereafter.
    - 5.1 Training will inform Payor Credentialing staff of:
        - 5.1.1 Organization audits of staff documentation and updates in credentialing files. Including understanding the audit process.
        - 5.1.2 The process for documenting and reporting inappropriate documentation and updates to:
            - 5.1.2.1 The organizations designated individual (s) when identified.
            - 5.1.2.2 NCQA, when the organization identifies fraud and misconduct.
        - 5.1.3 The consequences for inappropriate documentation and updates.

FILE RETENTION AND DESTRUCTION

1. Credentials files are retained indefinitely, either in paper or electronic format.
2. Paper files may be destroyed when the information/data contained in the paper file has been stored electronically.
3. Disposal of Confidential and Sensitive Data –
    - 3.1. See above Section 1. d. v. c. for disposal of electronic data.
    - 3.2. Printed confidential/sensitive data must be disposed of properly by confidential shredding.
    - 3.3. Confidential and sensitive paper material may also be placed in specialized collection bins that have been designated for that purpose. These special bins will be marked for confidential information disposal.

DATA RECOVERY and BACK-UP

1. Credentialing & Enrollment staff and Department shall be subject to and shall maintain compliance with the entire UVMHN Policy *INFOPOL3 Enterprise Data Backup and Retention Policy – See* Policy & The entire UVMHN Policy *UVMHN_INFO7 Information Technology Disaster Recover Policy- See Policy*.

SECURITY

1. Credentialing & Enrollment staff shall be subject to and shall maintain compliance with the entire UVMHN Policy UVMHN_INFO4 Information Security Program Policy, UVMHN_INFO5 Information User Security Policy & INFOPOL1Computer Room and Network Closet Access Policy for the Data Centers and Network Closets & -*See Policies.*

DEFINITIONS:

"Users" means UVMHN Staff including but not limited to, Network Director of Credentialing & Enrollment, Supervisors of Medical Staff and Payor Credentialing, Credentialing and Enrollment Specialists, Credentialing/Office Coordinators, Manager Business Applications, Application Analysts and any other reviewed and approved individuals that have a valid reason to need access to the UVMHN C&E Credentialing Software System.

"Credentialing & Enrollment Staff" means UVMHN C&E Staff including but not limited to, Network Director of Credentialing & Enrollment, Supervisors of Medical Staff and Payor Credentialing, Credentialing and Enrollment Specialists and Credentialing/Office Coordinators.

RELATED POLICIES:

C&E 8 Practitioner Confidentiality
C&E 10 Credentialing and Re-credentialing Processes
UVMHN Corrective Action Policy
INFOPOL3 Enterprise Data Backup and Retention Policy
INFOPOL1 Computer Room and Network Closet Access Policy for the Data Centers and Network Closets
UVMHN_INFO4 Information Security Program Policy
UVMHN_INFO5 Information Security User Policy
UVMHN_INFO7 Information Technology Disaster Recovery Policy

REFERENCES: National Committee for Quality Assurance

Date Reviewed/ Revised/Approved:	Restated/Reformatted from Credentials Plan approved: 9/24/2015, 9/13/2017, 9/6/2019, 06/19/2020, 02/19/2021, 12/17/2021, 01/21/2022, 02/17/2023, 02/16/2024, 02/21/2025

REVIEWERS: Michael D'Amico, MD Medical Director
Holly Turner, Network Director, MSS, Credentialing & Provider Enrollment

OWNER'S NAME: Holly Turner, CPCS, CPMSM, Network Director, MSS, Credentialing & Provider Enrollment

APPROVING OFFICIAL'S NAME: Michael D'Amico, MD Medical Director

Annual CR Information Integrity Assessment Reporting Tool

Description: An **annual** credentialing information integrity audit is required to be performed on credentialing verifications (CR 3), credentialing decisions (CR 2, CR 4) and ongoing monitoring (CR 5) for inappropriate documentation/updates. [If audit concludes noncompliant documentation or updates were identified then NCQA requires a reaudit (of that item) to be conducted within 3-6 months after the annual audit to determine the effectiveness of corrective actions implemented and conclude overall effectiveness of the actions taken. See additional tabs.]

Instructions: *An audit report is required to be completed even if there were no inappropriate documentation and updates identified.* ***Complete all the yellow highlighted fields and fields will unhighlight automatically. Use drop-down for light yellow highlighted field. All purple fields are set to auto-populate once other areas are completed (do not enter data into purple fields as it will remove the set formulas). If the cell has a*** *red* ***corner, the note will provide further direction in completing the field.*** *All of the information below is required to be completed* ***to meet the criterion and header information NCQA outlines under NCQA HP 2025 Standards, CR 8 Credentialing Information Integrity Element C and D.***

Organization Name:	.							**MSO Name:**	.
Auditor Name and Title:	.								
Audit Date/Report Date:	.							**File Methodology:**	5%/50 (Min. 10/10)
Audit Period (Look-back dates)**:**	.							**Adequate # Files:**	
Audit Universe (# I/R in look-back)**:**	**Initial #:**		**Recred #:**		**Total:**	0	**5% =:** 0	**Frequency:**	Annually
Sample Size (#'s audited)**:**	**Initial #:**		**Recred #:**		**Total Sample:**	0		**Required Sample:**	**Minimum 10/10**

The 5% sample review, (minimum of 10/10), requires both cred and recred files; divided as equally as possible from the look back period. *See note.*

Scoring Guide: ***Audit Sampling: 5% or 50 files (whichever is less) minimum of 10/10 of all initial credentialing and recredentialing decisions made or due in the previous calendar year.***
- ***Score "N/A": A documentation/update was made and the update was appropriate or there were no documentation or updates made.***
- ***Score "0": A documentation/update was made and the update was inappropriate. Details of findings are required.***

The review of items below should include checklists, systems, and files for ANY documentation or updates made that were inappropriate .

Inappropriate Documentation/ Updates to include are:
- ***Falsifying credentialing dates (e.g., licensure dates, credentialing decision dates, staff verifier dates, ongoing monitoring dates).***
- ***Creating documents without performing the required activities.***
- ***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.***

File Information			*File Review (CR 3)*								*Approval Process (CR 2)*		*Ongoing Monitoring Reports (CR 5)*			*Rationale for inappropriate documentation and updates*
File #	Practitioner ID	Initial / Recred	Application and Attestation	License	DEA / CDS	Education and Training	Board Certification	Work History	Malpractice History	Sanctions/Exclusions (State, M/M)	Credentialing Committee Minutes	Clean-file Approval, if applicable	Sanctions, Exclusions, Expirations Complaints/Adverse Events	Inappropriate Documentation or Updates?	**Credential Affected** (e.g. Application, Sanction Information, etc.) Please use concise language as space is limited.	**Findings/Comments** (See note for example.) Please use concise language as space is limited.
1															N/A	N/A
2															N/A	N/A
3															N/A	N/A
4															N/A	N/A
5															N/A	N/A
6															N/A	N/A
7															N/A	N/A
8															N/A	N/A
9															N/A	N/A
10															N/A	N/A
11															N/A	N/A
12															N/A	N/A
13															N/A	N/A
14															N/A	N/A
15															N/A	N/A
16															N/A	N/A
17															N/A	N/A
18															N/A	N/A
19															N/A	N/A
20															N/A	N/A
21															N/A	N/A
22															N/A	N/A
23															N/A	N/A
24															N/A	N/A
25															N/A	N/A
26															N/A	N/A
27															N/A	N/A
28															N/A	N/A
29															N/A	N/A
30															N/A	N/A
31															N/A	N/A
32															N/A	N/A
33															N/A	N/A
34															N/A	N/A
35															N/A	N/A
36															N/A	N/A
37															N/A	N/A
38															N/A	N/A
39															N/A	N/A
40															N/A	N/A
41															N/A	N/A
42															N/A	N/A
43															N/A	N/A
44															N/A	N/A
45															N/A	N/A
46															N/A	N/A
47															N/A	N/A
48															N/A	N/A
49															N/A	N/A
50															N/A	N/A

# Compliant (N/A)	0	0	0	0	0	0	0	0	0	0	0
# Non-Compliant	0	0	0	0	0	0	0	0	0	0	0
# of Files Reviewed	0	0	0	0	0	0	0	0	0	0	0
% of Non-compliant Modifications	**N/A**	**N/A**	**N/A**	**N/A**	**N/A**	**N/A**	**N/A**	**N/A**	**N/A**	**N/A**	**N/A**

Credentialing Information Integrity (CII) Audit and Analysis Tool

GUIDE ON HOW TO COMPLETE

Key notes:

- *Cred Info Integrity Audit and Analysis Tool* ***REPLACES*** *Credentialing System Controls Annual Audit Report* and *Noncompliant Modifications Details Report.*
- The CII tool is both an audit and analysis report and contains all NCQA required information.
- CII audit is to be conducted annually.
- CII report needs to be completed even if there were no inappropriate documentation or updates.
- Advanced system control capabilities does not apply, and everyone is required to audit.
- The file sample is from files processed within your look back period (12 months). You are not assessing your entire system, full network roster or any/all modifications made within your system or files.

Save a blank/original copy of the CII audit and analysis tool as a reference.

Key notes (continued):

- The tool calculates your required sample size based on the number of files you have processed.
- Tool contains several “red corner” which indicates a note is in the cell to guide you on the information that is needed. Hover over the cell to review note.
- The yellow highlighted cells require manual entry, enter N/A if not applicable (e.g., MSO field).
- The lilac highlighted cells auto populate based on entries from other cells. Do not override.
- Always use the “back/undo” button if you made an error.

Key notes (continued):

There are four (4) tabs to this report:

- *CII Audit*
- *CII Analysis*
- *ReAudit Tool*
- *Effectiveness of Actions*

Upon Completion:

- If no inappropriate documentation or updates have been identified; you will complete the first two (2) tabs [CII Audit; CII Analysis (header only)] and STOP.
- If inappropriate documentation or updates have been identified; you will need to do a reaudit within 3-6 months by completing the 3rd and 4th tab [ReAudit Tool; Effectiveness of Actions].

Sample methodology of files and tool calculations.

1.

Audit Universe (# I/R in look-back):	Initial #:	8	Recred #:	30	Total:	38	5% =:	2	Frequency: Annually	
Sample Size (#'s audited):	Initial #:	8	Recred #:	10	Total Sample:		18		Required Sample:	Minimum 10/10

2.

Audit Universe (# I/R in look-back):	Initial #:	250	Recred #:	340	Total:	590	5% =:	30	Frequency: Annually	
Sample Size (#'s audited):	Initial #:	15	Recred #:	15	Total Sample:		30		Required Sample:	5% (Max of 50)

3.

Audit Universe (# I/R in look-back):	Initial #:	100	Recred #:	130	Total:	230	5% =:	12	Frequency: Annually	
Sample Size (#'s audited):	Initial #:	10	Recred #:	10	Total Sample:		20		Required Sample:	Minimum 10/10

4.

Audit Universe (# I/R in look-back):	Initial #:	458	Recred #:	932	Total:	1390	5% =:	70	Frequency: Annually	
Sample Size (#'s audited):	Initial #:	25	Recred #:	25	Total Sample:		50		Required Sample:	5% (Max of 50)

1. 5% = 2 files. Minimum required is 10 initial and 10 recred. Must pull all 8 initial and 10 recred.

2. 5% = 30 files. Required is the 30 files. Select 15 initial and 15 recred. (equally divide b/w initial and recred)

3. 5% = 12 files. Minimum required is 10 initial and 10 recred. Must pull 10 initial and 10 recred.

4. 5%= 70 files. Max number of files is 50. Select 25 initial and 25 recred. (equally divide b/w initial and recred)

If 5% equals 20 files or less, then required to use the "minimum" methodology which is 10 initial/10 recred.
If you do not have at least 10 initial or 10 recred, audit all that are available.
Equally divide the file sampling against the initial and recred, unless files limited.

Example of a completed audit tool with **NO** identified inappropriate documentation or updates.

CII Audit Tab

Organization Name: Enter PO name

MSO Name: Enter MSO name or N/A

Auditor and Title: Enter the name and title of person conducting the CII audit

Audit Date/Report Date: Enter the date(s) the CII audit is conducted.

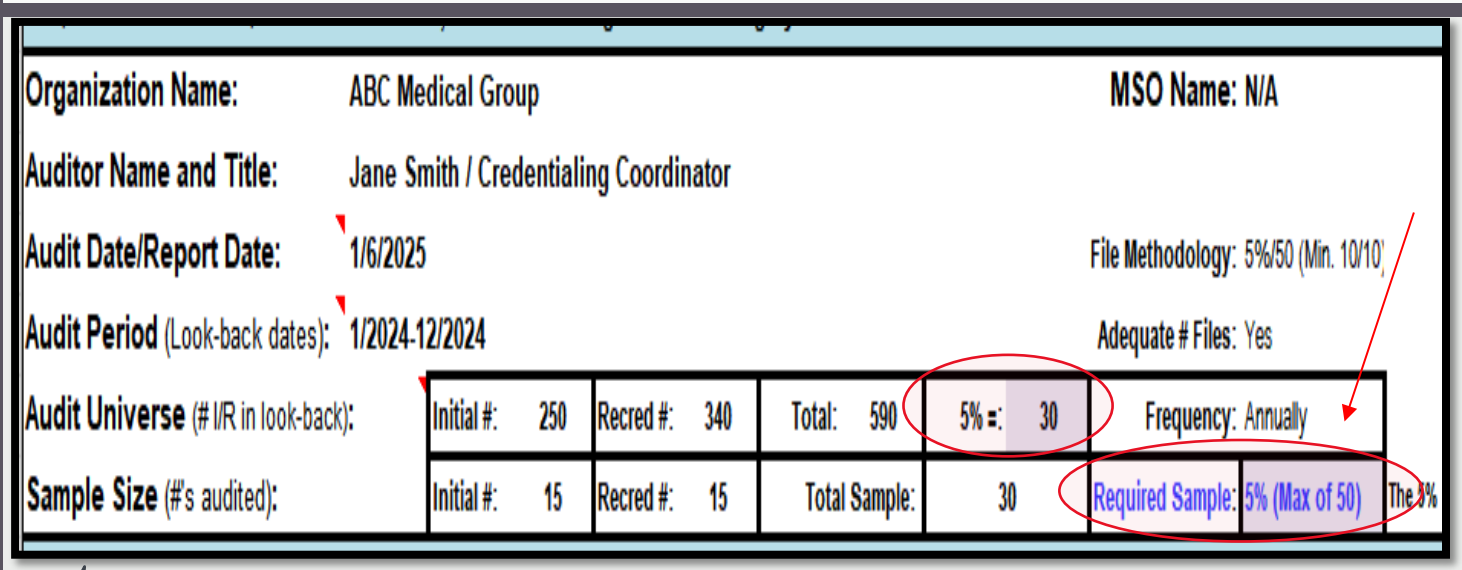
Audit Period: This is the timeframe of files you are reviewing with a 12 month look back from your audit date.

Audit Universe: Enter the number of initial cred files and recred files you have credentialed during the audit period.

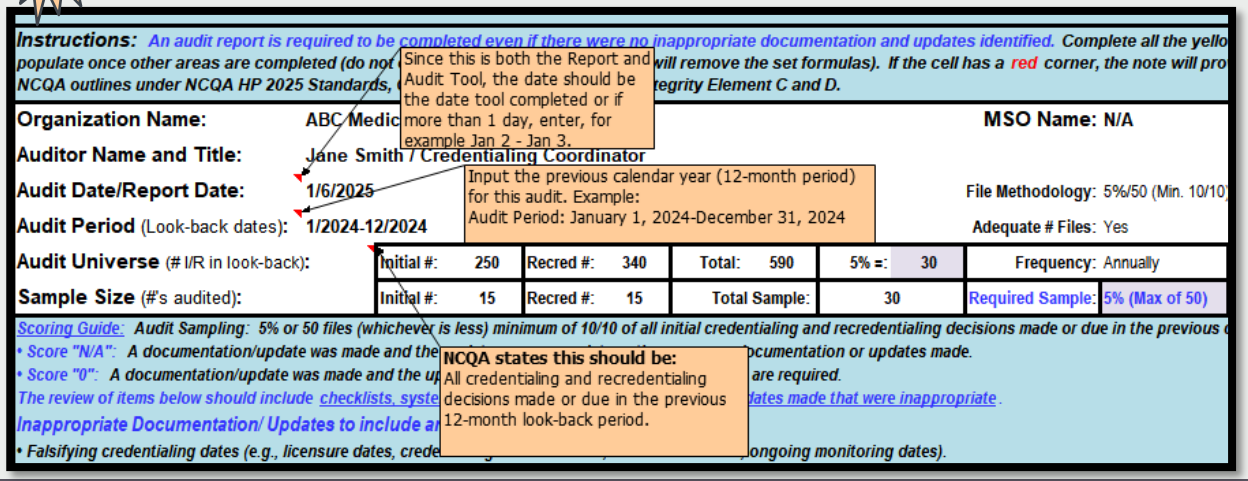
5%=: This cell will calculate the 5% based on totals in your audit universe.

Required Sample: Will indicate the sampling size to follow. Either minimum (10/10) or 5% (Max of 50).

Sample Size: Enter in the # of initial and recred files audited. This must meet the required sample size.



Hover over the "red corners" you will see the explanation of what is needed for each cell.



Adequate # Files – use drop down to indicate if there was an adequate # of files selected. If not, chose option.

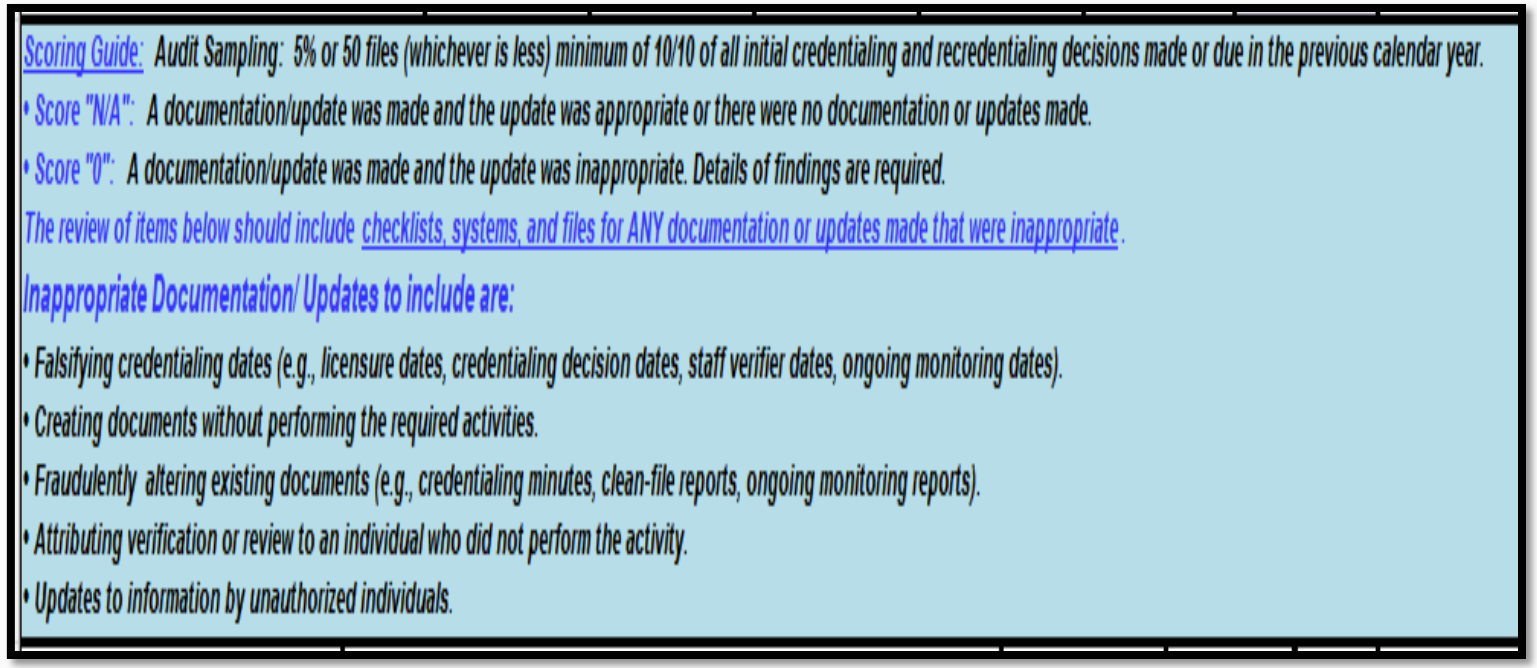
Scoring Guide

The tool has drop downs to select “N/A” or “0” for each credentialing element.

Score “N/A”: When a documentation or update was made that *was appropriate* or if there were *no documentation or updates* made to the credentialing information

Score “0”: When a documentation or update was made that *was inappropriate* to the credentialing information.

Remember: You are reviewing each credentialing element against checklist, systems, files for any inappropriate documentation or updates.



Scoring Guide: Audit Sampling: 5% or 50 files (whichever is less) minimum of 10/10 of all initial credentialing and recredentialing decisions made or due in the previous calendar year.

- Score "N/A": A documentation/update was made and the update was appropriate or there were no documentation or updates made.
- Score "0": A documentation/update was made and the update was inappropriate. Details of findings are required.

The review of items below should include checklists, systems, and files for ANY documentation or updates made that were inappropriate.

Inappropriate Documentation/ Updates to include are:

- Falsifying credentialing dates (e.g., licensure dates, credentialing decision dates, staff verifier dates, ongoing monitoring dates).
- Creating documents without performing the required activities.
- 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.

File information: Enter the practitioner ID (name, unique system ID, NPI, initials, etc.)
Initial/Recred: Use drop down to select if the file is an initial file or a recred file.

File Review: Each credentialing element is listed. Use the scoring guide to determine if "N/A" or "0" applies.

Approval Process:
Review the files against the Credentialing Minutes and Clean file process (if applicable).

Ongoing Monitoring:
Review the files against the Ongoing Monitoring Reports.

File Information			File Review (CR 3)								Approval Process (CR 2)		Ongoing Monitoring Reports (CR 5)			Rationale for inappropriate documentation and updates
File #	Practitioner ID	Initial / Recred	Application and Attestation	License	DEA / CDS	Education and Training	Board Certification	Work History	Malpractice History	Sanctions/Exclusions (State, M/M)	Credentialing Committee Minutes	Clean-file Approval, if applicable	Sanctions, Exclusions, Expirations Complaints/Adverse Events	Inappropriate Documentation or Updates?	Credential Affected (e.g. Application, Sanction Information, etc.) Please use concise language as space is limited.	Findings/Comments (See note for example.) Please use concise language as space is limited.
1	Smith	Initial	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	No	N/A	N/A
2	Richardson	Recred	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	No	N/A	N/A

Inappropriate documentation or updates field will automatically enter a "yes/no" based on you completing the review of each file. All fields must be completed.

Credential Affected and Finding/Comments:
Will remain "N/A", as there were no inappropriate documentation or updates identified.

CII Analysis Tab

Move on to the CII Analysis Tab
The information that was entered on the CII audit tab will automatically pull into this tab.

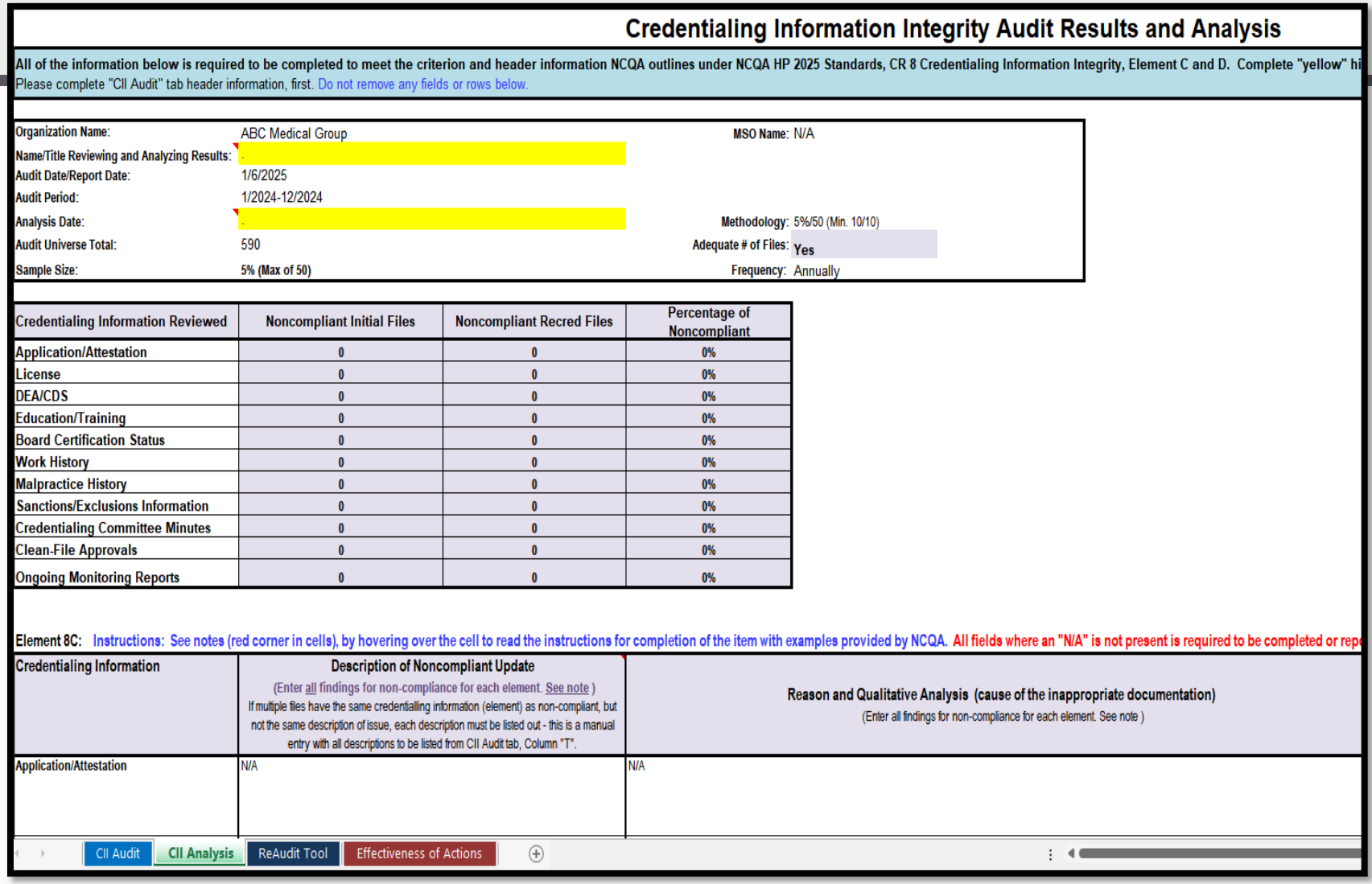
Complete the “yellow fields”

Name/Title Reviewing and Analyzing Results:

- This may be the same person who conducted the CII audit or another individual who reviewed the results.

Analysis Date:

- This is the date the CII audit was analyzed. It may be the same date as the CII audit or may differ if someone additional is reviewing.



Credentialing Information Integrity Audit Results and Analysis

All of the information below is required to be completed to meet the criterion and header information NCQA outlines under NCQA HP 2025 Standards, CR 8 Credentialing Information Integrity, Element C and D. Complete "yellow" hi
Please complete "CII Audit" tab header information, first. Do not remove any fields or rows below.

Organization Name:	ABC Medical Group	MSO Name:	N/A
Name/Title Reviewing and Analyzing Results:	.		
Audit Date/Report Date:	1/6/2025		
Audit Period:	1/2024-12/2024		
Analysis Date:	.	Methodology:	5%/50 (Min. 10/10)
Audit Universe Total:	590	Adequate # of Files:	Yes
Sample Size:	5% (Max of 50)	Frequency:	Annually

Credentialing Information Reviewed	Noncompliant Initial Files	Noncompliant Recred Files	Percentage of Noncompliant
Application/Attestation	0	0	0%
License	0	0	0%
DEA/CDS	0	0	0%
Education/Training	0	0	0%
Board Certification Status	0	0	0%
Work History	0	0	0%
Malpractice History	0	0	0%
Sanctions/Exclusions Information	0	0	0%
Credentialing Committee Minutes	0	0	0%
Clean-File Approvals	0	0	0%
Ongoing Monitoring Reports	0	0	0%

Element 8C: Instructions: See notes (red corner in cells), by hovering over the cell to read the instructions for completion of the item with examples provided by NCQA. All fields where an "N/A" is not present is required to be completed or rep

Credentialing Information	Description of Noncompliant Update (Enter all findings for non-compliance for each element. See note) If multiple files have the same credentialling information (element) as non-compliant, but not the same description of issue, each description must be listed out - this is a manual entry with all descriptions to be listed from CII Audit tab, Column "T".	Reason and Qualitative Analysis (cause of the inappropriate documentation) (Enter all findings for non-compliance for each element. See note)
Application/Attestation	N/A	N/A

CII Audit | CII Analysis | ReAudit Tool | Effectiveness of Actions

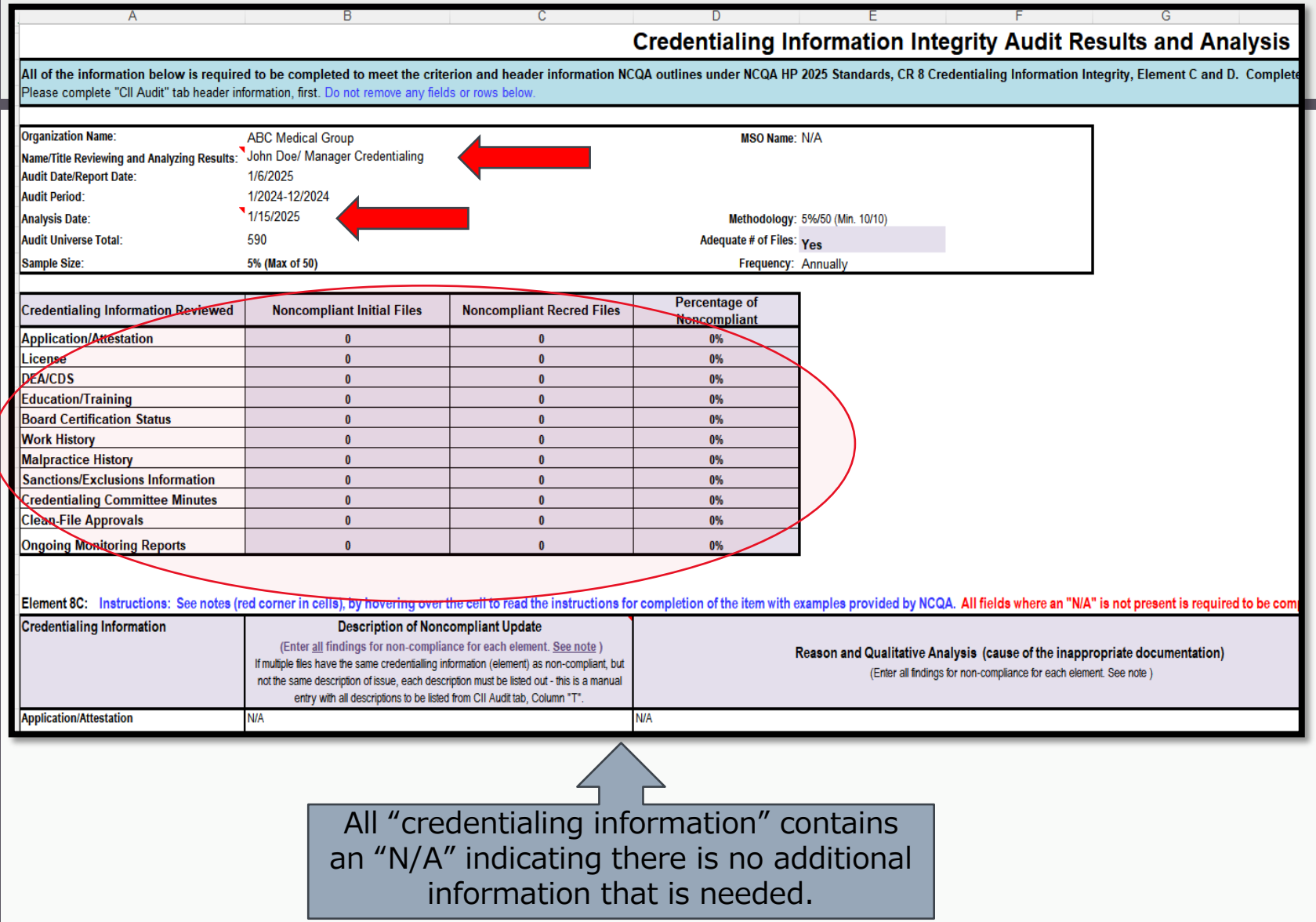
Compliance grid:

This grid will auto populate based on the audit data entries on the CII audit tab. It will calculate the percentage of noncompliance for each initial and recred element.

- "0"'s are GOOD here!

STOP! YOUR CII Audit and Analysis is complete for the YEAR!

Nothing further is needed since there was no inappropriate documentation or updates identified during the CII audit.



Credentialing Information Integrity Audit Results and Analysis

All of the information below is required to be completed to meet the criterion and header information NCQA outlines under NCQA HP 2025 Standards, CR 8 Credentialing Information Integrity, Element C and D. Complete
Please complete "CII Audit" tab header information, first. Do not remove any fields or rows below.

Organization Name:	ABC Medical Group	MSO Name:	N/A
Name/Title Reviewing and Analyzing Results:	John Doe/ Manager Credentialing		
Audit Date/Report Date:	1/6/2025		
Audit Period:	1/2024-12/2024		
Analysis Date:	1/15/2025	Methodology:	5%/50 (Min. 10/10)
Audit Universe Total:	590	Adequate # of Files:	Yes
Sample Size:	5% (Max of 50)	Frequency:	Annually

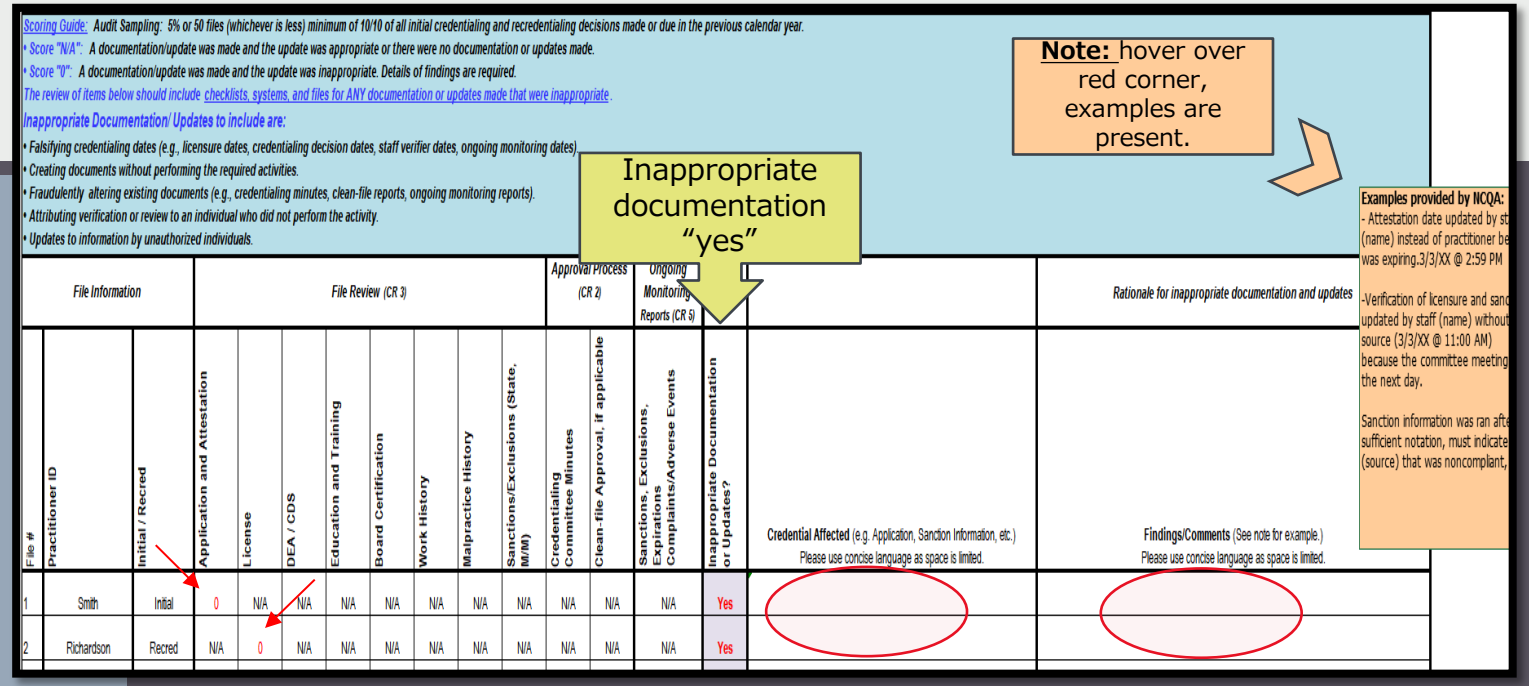
Credentialing Information Reviewed	Noncompliant Initial Files	Noncompliant Recred Files	Percentage of Noncompliant
Application/Attestation	0	0	0%
License	0	0	0%
DEA/CDS	0	0	0%
Education/Training	0	0	0%
Board Certification Status	0	0	0%
Work History	0	0	0%
Malpractice History	0	0	0%
Sanctions/Exclusions Information	0	0	0%
Credentialing Committee Minutes	0	0	0%
Clean File Approvals	0	0	0%
Ongoing Monitoring Reports	0	0	0%

Element 8C: Instructions: See notes (red corner in cells), by hovering over the cell to read the instructions for completion of the item with examples provided by NCQA. All fields where an "N/A" is not present is required to be com

Credentialing Information	Description of Noncompliant Update (Enter all findings for non-compliance for each element. See note) If multiple files have the same credentialling information (element) as non-compliant, but not the same description of issue, each description must be listed out - this is a manual entry with all descriptions to be listed from CII Audit tab, Column "T".	Reason and Qualitative Analysis (cause of the inappropriate documentation) (Enter all findings for non-compliance for each element. See note)
Application/Attestation	N/A	N/A

All "credentialing information" contains an "N/A" indicating there is no additional information that is needed.

Example of a completed audit tool **WITH** identified inappropriate documentation and updates.



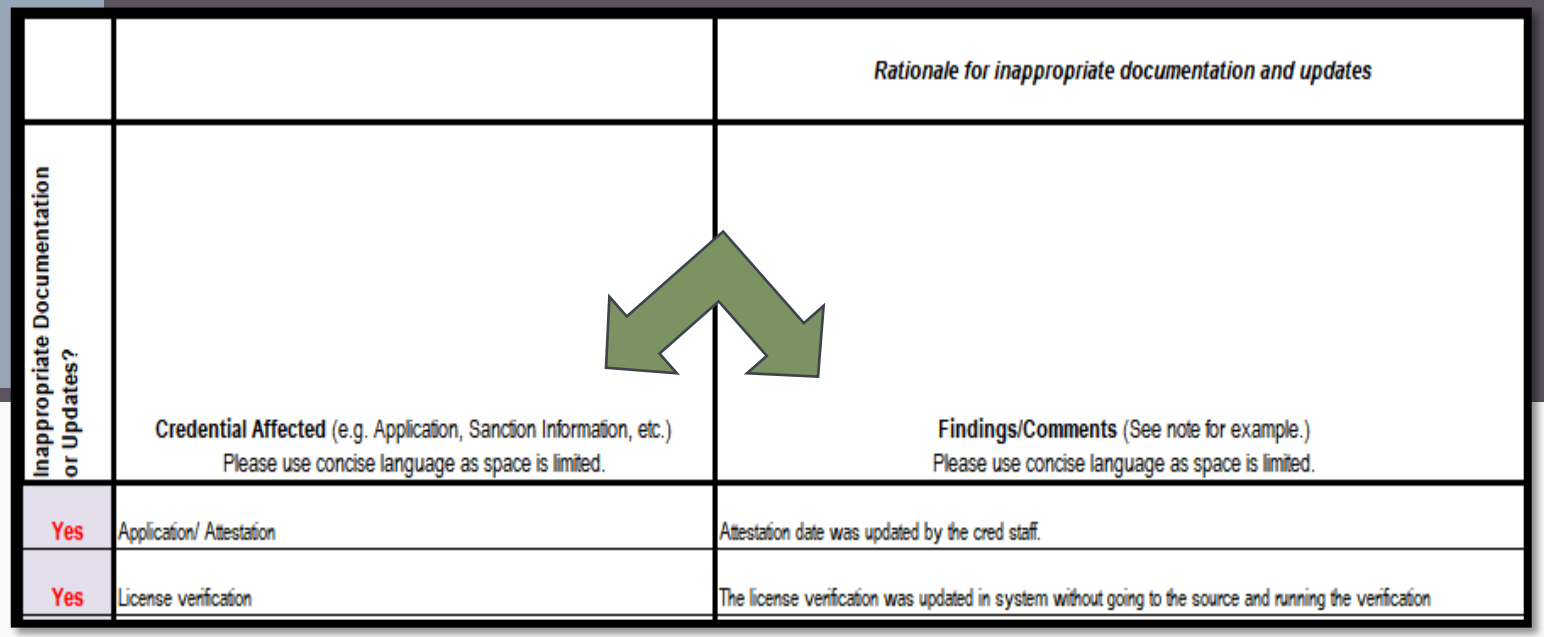
Scoring Guide: Audit Sampling: 5% or 50 files (whichever is less) minimum of 10/10 of all initial credentialing and recredentialing decisions made or due in the previous calendar year.
• Score "N/A": A documentation/update was made and the update was appropriate or there were no documentation or updates made.
• Score "0": A documentation/update was made and the update was inappropriate. Details of findings are required.
The review of items below should include checklists, systems, and files for ANY documentation or updates made that were inappropriate.
Inappropriate Documentation/ Updates to include are:
• Falsifying credentialing dates (e.g., licensure dates, credentialing decision dates, staff verifier dates, ongoing monitoring dates).
• Creating documents without performing the required activities.
• 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.

Note: hover over red corner, examples are present.

Inappropriate documentation "yes"

Examples provided by NCQA:
- Attestation date updated by st (name) instead of practitioner be was expiring.3/3/XX @ 2:59 PM
-Verification of licensure and sanc updated by staff (name) without source (3/3/XX @ 11:00 AM) because the committee meeting the next day.
Sanction information was ran afte sufficient notation, must indicate (source) that was noncompliant,

File Information			File Review (CR 3)								Approval Process (CR 2)		Ongoing Monitoring Reports (CR 5)		Rationale for inappropriate documentation and updates	
File #	Practitioner ID	Initial / Recred	Application and Attestation	License	DEA / CDS	Education and Training	Board Certification	Work History	Malpractice History	Sanctions/Exclusions (State, M/M)	Credentialing Committee Minutes	Clean-file Approval, if applicable	Sanctions, Exclusions, Expirations Complaints/Adverse Events	Inappropriate Documentation or Updates?	Credential Affected (e.g. Application, Sanction Information, etc.) Please use concise language as space is limited.	Findings/Comments (See note for example.) Please use concise language as space is limited.
1	Smith	Initial	0	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Yes		
2	Richardson	Recred	N/A	0	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Yes		



Inappropriate Documentation or Updates?	Credential Affected (e.g. Application, Sanction Information, etc.) Please use concise language as space is limited.	Rationale for inappropriate documentation and updates: Findings/Comments (See note for example.) Please use concise language as space is limited.
Yes	Application/ Attestation	Attestation date was updated by the cred staff.
Yes	License verification	The license verification was updated in system without going to the source and running the verification

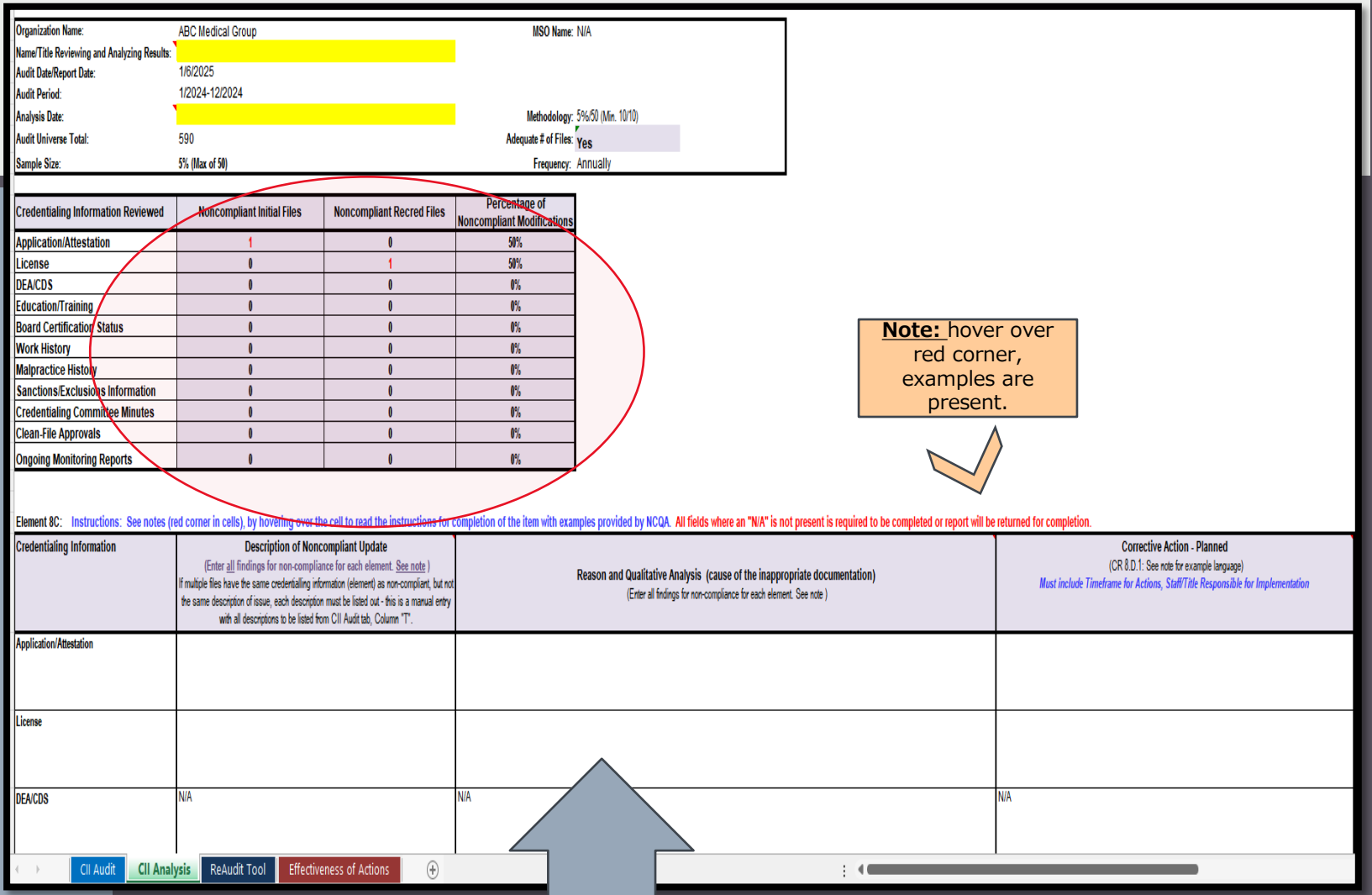
Scoring: Enter "0" in the credentialing information that was found to have an inappropriate documentation or update.

Inappropriate Documentation or Update Column: Will change to "yes"

Credentials Affected and Findings Comment Columns: If a "0" is entered, it will remove "N/A" from these fields and require additional information.

Credentials Affected: Enter the credentialing element that had an inappropriate documentation or update.

Findings/Comments: Enter the issue that was identified. *(See red corner note!)*



Organization Name:	ABC Medical Group	MSO Name: N/A	
Name/Title Reviewing and Analyzing Results:			
Audit Date/Report Date:	1/6/2025		
Audit Period:	1/2024-12/2024		
Analysis Date:		Methodology: 5%/50 (Min. 10/10)	
Audit Universe Total:	590	Adequate # of Files: Yes	
Sample Size:	5% (Max of 50)	Frequency: Annually	

Credentialing Information Reviewed	Noncompliant Initial Files	Noncompliant Recred Files	Percentage of Noncompliant Modifications
Application/Attestation	1	0	50%
License	0	1	50%
DEA/CDS	0	0	0%
Education/Training	0	0	0%
Board Certification Status	0	0	0%
Work History	0	0	0%
Malpractice History	0	0	0%
Sanctions/Exclusions Information	0	0	0%
Credentialing Committee Minutes	0	0	0%
Clean-File Approvals	0	0	0%
Ongoing Monitoring Reports	0	0	0%

Note: hover over red corner, examples are present.

Element 8C: Instructions: See notes (red corner in cells), by hovering over the cell to read the instructions for completion of the item with examples provided by NCQA. All fields where an "N/A" is not present is required to be completed or report will be returned for completion.

Credentialing Information	Description of Noncompliant Update (Enter all findings for non-compliance for each element. See note) If multiple files have the same credentialing information (element) as non-compliant, but not the same description of issue, each description must be listed out - this is a manual entry with all descriptions to be listed from CII Audit tab, Column "I".	Reason and Qualitative Analysis (cause of the inappropriate documentation) (Enter all findings for non-compliance for each element. See note)	Corrective Action - Planned (CR 8.D.1: See note for example language) Must include Timeframe for Actions, Staff/Title Responsible for Implementation
Application/Attestation			
License			
DEA/CDS	N/A	N/A	N/A

CII Audit | CII Analysis | ReAudit Tool | Effectiveness of Actions

These three fields are now "blank" as the N/A's will automatically be removed indicating additional information is needed.

Move on to the CII Analysis Tab
The information that was entered on the CII audit tab will automatically pull into this tab.

- Complete the "yellow fields"

Name/Title Reviewing and Analyzing Results:

- This may be the same person who conducted the CII audit or another individual who reviewed the results.

Analysis Date:

- This is the date the CII audit was analyzed. It may be the same date as the CII audit or may differ if someone additional is reviewing.

Compliance grid: This grid will auto populate based on the audit data entries on the CII audit tab. It will calculate the percentage of noncompliance for each initial and recred element.

Credentialing Information	Description of Noncompliant Update (Enter all findings for non-compliance for each element. See note) If multiple files have the same credentialling information (element) as non-compliant, but not the same description of issue, each description must be listed out - this is a manual entry with all descriptions to be listed from CII Audit tab, Column "I".	Reason and Qualitative Analysis (cause of the inappropriate documentation) (Enter all findings for non-compliance for each element. See note)	Corrective Action - Planned (CR 8.D.1: See note for example language) *Must include Timeframe for Actions, Staff/Title Responsible for Implementation*
Application/Attestation	Attestation date was updated by the cred staff.	Staff spoke with the practitioner, who stated that all information remained accurate. Staff did not know that only the practitioner can update the information.	Educate staff on the CII policies by 2/1/2025 Train staff on NCQA's documentation requirements by 2/1/2025 Establish automated resending of attestation to practitioner 60 days before expiration by 3/1/2025 * Credentialing Manager responsible for implementation of these actions
License	The license verification was updated in system without going to the source and running the verification	Staff responsible for verification of licensure and sanction information was on emergency leave and did not complete verification. Temporary staff did not have time to complete verification of all practitioners, they copied existing credentials, changed dates and uploaded the information into the CR system before the Credentialing Committee meeting.	Require credentialing staff to undergo ethics training, with emphasis on following organization processes even if under pressure to take shortcuts. by 2/1/2025 - Purchase software application to automatically retrieve verification from accepted sources (web crawler) by 3/1/2025 *Credentialing Manager and IT Director responsible for implementation

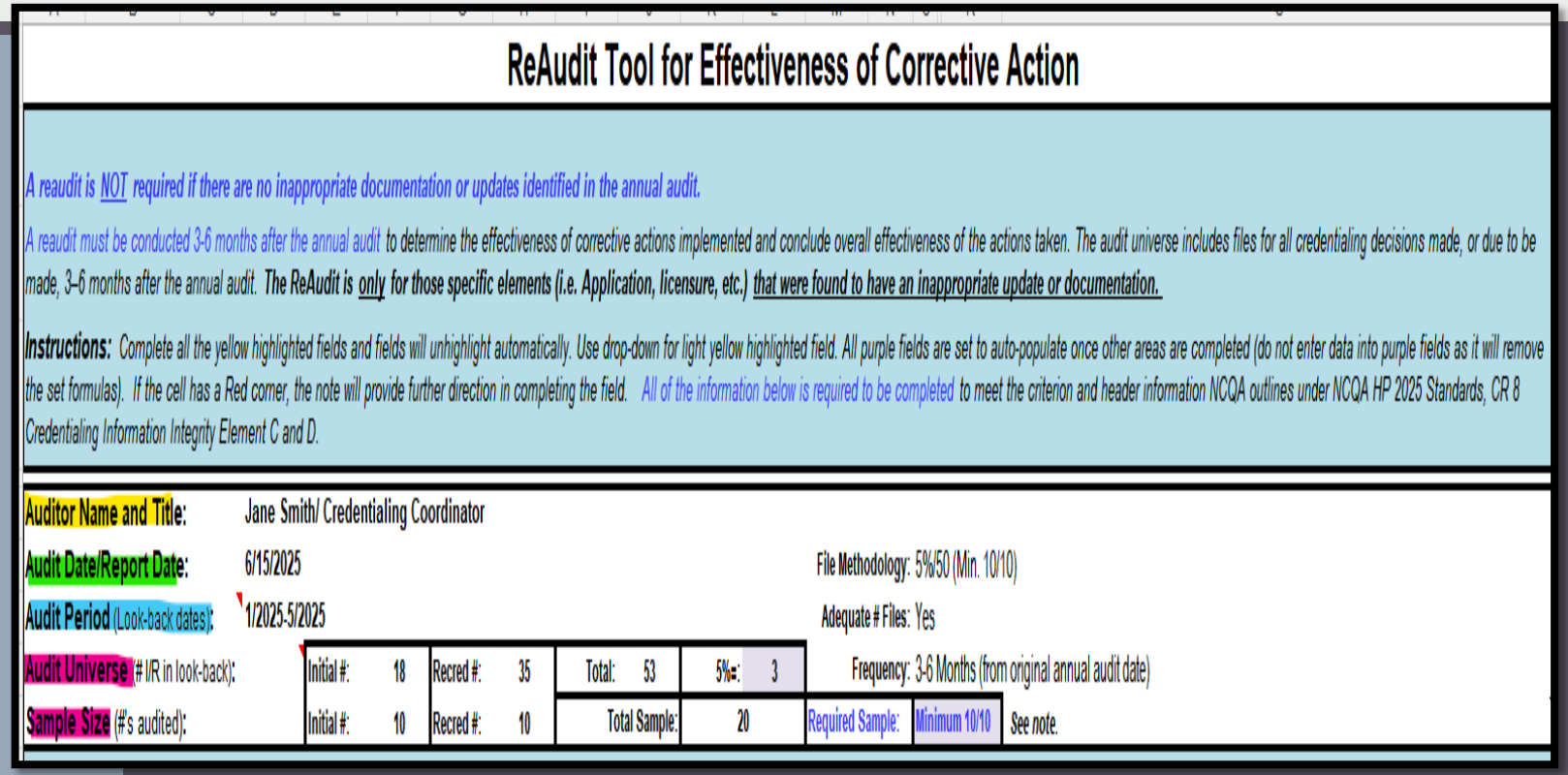
Description of Noncompliant Update: Manual entry, describe the issue that was identified (align with the comment on the CII audit tab).

Reason and Qualitative Analysis: Include the reason and the qualitative analysis for each finding. *An examination of the underlying reason for or cause of results, including deficiencies or processes that may present barriers to improvement or cause failure to reach a stated goal. Qualitative analysis draws conclusions about why the results, are what they are and involves staff responsible for executing a program or process. Also called a causal, root cause or barrier analysis.*

Corrective Action Planned: Include the ***planned actions*** for correction, the ***timeframe*** for actions and the ***staff/title*** who is responsible for implementation.

Take this time to implement the corrective actions. A re-audit is required in 3-6 months

3-6 months from the CII audit, a Reaudit is required!



ReAudit Tool for Effectiveness of Corrective Action

A reaudit is NOT required if there are no inappropriate documentation or updates identified in the annual audit.

A reaudit must be conducted 3-6 months after the annual audit to determine the effectiveness of corrective actions implemented and conclude overall effectiveness of the actions taken. The audit universe includes files for all credentialing decisions made, or due to be made, 3–6 months after the annual audit. ***The ReAudit is only for those specific elements (i.e. Application, licensure, etc.) that were found to have an inappropriate update or documentation.***

Instructions: *Complete all the yellow highlighted fields and fields will unhighlight automatically. Use drop-down for light yellow highlighted field. All purple fields are set to auto-populate once other areas are completed (do not enter data into purple fields as it will remove the set formulas). If the cell has a Red corner, the note will provide further direction in completing the field. All of the information below is required to be completed to meet the criterion and header information NCQA outlines under NCQA HP 2025 Standards, CR 8 Credentialing Information Integrity Element C and D.*

Auditor Name and Title:	Jane Smith/ Credentialing Coordinator								
Audit Date/Report Date:	6/15/2025					File Methodology: 5%/50 (Min. 10/10)			
Audit Period (Look-back dates):	1/2025-5/2025					Adequate # Files: Yes			
Audit Universe (# I/R in look-back):	Initial #:	18	Recred #:	35	Total: 53	5%=: 3	Frequency: 3-6 Months (from original annual audit date)		
Sample Size (#'s audited):	Initial #:	10	Recred #:	10	Total Sample:	20	Required Sample:	Minimum 10/10	*See note.*

Audit Name/Title: Person/title conducting the reaudit.

Audit date/report date: Date the reaudit is conducted.

Audit period: Audit period is now from the timeframe of the original CII audit to date of reaudit.

Audit Universe: # of initial and recred files processed during the previous 3–6-month audit period.

Sample size: How many files did you select for the audit.

Refer to slide 6 if you need further instructions on sample size.

- The tool will identify the sample size.
- The audit universe is the timeframe since the original CII audit.

Scoring Guide: Audit Sampling: 5% or 50 files (whichever is less) minimum of 10/10 of all initial credentialing and recredentialing decisions made or due in the previous 3-6 months.
- Score "N/A": A documentation/update was made and the update was appropriate or there were no documentation or updates made.
- Score "0": A documentation/update was made and the update was inappropriate. Details of findings are required.

The review of items below should include checklists, system and files for ANY documentation or updates made that were inappropriate. "N/R"= Not Required (based on original audit, the element is not required to be reviewed, again)

File Information			File Review (CR 3)								Approval Process (CR 2)		Ongoing Monitoring (CR 5)		
File #	Practitioner ID	Initial / Recred	~~Application and Attestation~~	~~License~~	DEA / CDS	Education and Training	Board Certification	Work History	Malpractice History	Sanctions/Exclusions (State, M/M)	Credentialing Committee Minutes	Clean-file Approval, if applicable	Sanctions, Exclusions, Expirations Complaints/Adverse Events	Inappropriate Documentation or Updates?	Credential Affected (e.g. Application, Sanction Information, etc.)
1					N/R	N/R	N/R	N/R	N/R	N/R	N/R	N/R	N/R	No	N/A
2					N/R	N/R	N/R	N/R	N/R	N/R	N/R	N/R	N/R	No	N/A

Reaudit: You are only required to review the credentialing information that had inappropriate documentation or updates during the original CII audit.

Note in example, the application/attestation and license fields have "opened up" for review, while the remaining credentialing element cells contain a "N/R" = Not required

Scoring Guide: Audit Sampling: 5% or 50 files (whichever is less) minimum of 10/10 of all initial credentialing and recredentialing decisions made or due in the previous 3-6 months.
- Score "N/A": A documentation/update was made and the update was appropriate or there were no documentation or updates made.
- Score "0": A documentation/update was made and the update was inappropriate. Details of findings are required.

The review of items below should include checklists, system and files for ANY documentation or updates made that were inappropriate. "N/R"= Not Required (based on original audit, the element is not required to be reviewed, again)

File Information			File Review (CR 3)								Approval Process (CR 2)		Ongoing Monitoring (CR 5)		
File #	Practitioner ID	Initial / Recred	Application and Attestation	License	DEA / CDS	Education and Training	Board Certification	Work History	Malpractice History	Sanctions/Exclusions (State, M/M)	Credentialing Committee Minutes	Clean-file Approval, if applicable	Sanctions, Exclusions, Expirations Complaints/Adverse Events	Inappropriate Documentation or Updates?	Credential Affected (e.g. Application, Sanction Information, etc.)
1	Jennings	Initial	N/A	N/A	N/R	N/R	N/R	N/R	N/R	N/R	N/R	N/R	N/R	No	N/A
2	Flemming	Recred	N/A	N/A	N/R	N/R	N/R	N/R	N/R	N/R	N/R	N/R	N/R	No	N/A

Score guide: Score element as "N/A" or "0".

Once the Reaudit tool tab is completed, move to the Effectiveness of Actions tab to close out and draw conclusions of the corrective actions and reaudit.

Organization Name:	ABC Medical Group	MSO Name: N/A	
Name/Title Reviewing/Analyzing Results:	John Doe/ Manager Credentialing		
Audit Date:/Report Date:	6/15/2025		
Audit Period	1/2025-5/2025		
Analysis Date:	6/16/2025	Methodology: 5%/50 (Min. 10/10)	
Sample Size	Minimum 10/10		

Credentialing Information Reviewed	Noncompliant Initial Files	Noncompliant Recred Files	Percentage of Noncompliant Modifications
Application/Attestation	0	0	0%
License	0	0	0%
DEA/CDS	0	0	N/A
Education/Training	0	0	N/A
Board Certification Status	0	0	N/A
Work History	0	0	N/A
Malpractice History	0	0	N/A
Sanctions/Exclusions Information	0	0	N/A
Credentialing Committee Minutes	0	0	N/A
Clean-File Approvals	0	0	N/A
Ongoing Monitoring Reports	0	0	N/A

Element 8C: Instructions: Shaded column will auto-populate from other tab. All fields where an "N/A" is not present is required to be completed or report will be returned for completion based on that specific cred information. See notes for examples (red corner).

Credentialing Information	ORIGINAL Description of Noncompliant Update	Corrective Actions - Completed (Include date)	Conclusion (Identify if reaudit showed compliance, if not, identify if any deficiencies found in reaudit.) (Action Effectiveness Audit) An overall conclusion must be made and populated in Row 51.
Application/Attestation	Attestation date was updated by the cred staff.	All staff completed education on the CII policies and NCQA's documentation requirements on 1/30/2025. Establish automated process for resending of attestation to practitioner 60 days before expiration; completed on 2/25/2025.	These actions have eliminated updating of attestation by the credentialing staff. There were no additional incidences identified in the reaudit.
License	The license verification was updated in system without going to the source and running the verification	Credentialing staff completed ethics training, including our process on shortcuts on 1/30/2025. Software was for the credentialing system automatically retrieve verification from accepted sources (web crawler) on 2/25/2025 and program was up and running on 3/1/2025.	The actions have eliminated credentialing files being put through to committee without the actual primary source verifications of licensure being completed appropriately and timely. There were no additional incidences identified in the reaudit.
DEA/CDS	N/A	N/A	N/A

Overall Effectiveness – Conclusion: manual entry into this cell, on the conclusion of the reaudit.

50	***Overall Effectiveness-Conclusion:*** NCQA requires an overall statement to confirm effectiveness of correction actions implemented. See note in cell A50 and complete your summary conclusion in the box.
51	The corrective actions implemented have been effective in preventing inappropriate documentation and updates to the credentialing information based on follow-up audit and assessment. There were no additional incidences of inappropriate documentation and updates made.
52	
53	
54	
55	
56	
57	

Complete: Name/Title Reviewing/ Analyzing report *and* Analysis Date

Compliance Grid: The grid data will pull over based on the ReAudit tab.

Corrective Actions-Completed Document the actions that were taken and the date they were completed.

Conclusion: Enter the conclusion for each credentialing element based on the implemented action plan and reaudit results

STOP! CII audit and Reaudit complete! Next audit due 12 months from the annual CII audit.

ReAudit – Identified inappropriate documentation and updates.

New or previous issues identified during the reaudit:

Identify noncompliance by scoring "0"

Inappropriate Documentation will change to "yes"

File Information			File Review (CR 3)								Approval Process (CR 2)		Ongoing Monitoring (CR 5)		
File #	Practitioner ID	Initial / Recred	Application and Attestation	License	DEA / CDS	Education and Training	Board Certification	Work History	Malpractice History	Sanctions/Exclusions (State, M/M)	Credentialing Committee Minutes	Clean-file Approval, if applicable	Sanctions, Exclusions, Expirations Complaints/Adverse Events	Inappropriate Documentation or Updates?	Credential Affected (e.g. Application, Sanction Information, etc.)
1	Jennings	Initial	0	N/A	N/R	N/R	N/R	N/R	N/R	N/R	N/R	N/R	N/R	Yes	Application/ Attestation
2	Flemming	Recred	N/A	N/A	N/R	N/R	N/R	N/R	N/R	N/R	N/R	N/R	N/R	No	N/A

Credential Affected: Manual entry of credentialing element.

Credentialing Information	ORIGINAL Description of Noncompliant Update	Corrective Actions - Completed (Include date)	Conclusion (Identify if reaudit showed compliance, if not, identify if any deficiencies found in reaudit.) (Action Effectiveness Audit) An overall conclusion must be made and populated in Row 51.
Application/Attestation	Attestation date was updated by the cred staff.	All staff completed education on the CII policies and NCQA's documentation requirements on 1/30/2025. Establish automated process for resending of attestation to practitioner 60 days before expiration; completed on 2/25/2025.	These actions implemented have not eliminated updating of attestation by the credentialing staff. There was one additional findings of inappropriate documentation and update that was made to the application/ attestation.
License	The license verification was updated in system without going to the source and running the	Credentialing staff completed ethics training, including our process on shortcuts on	The actions have eliminated credentialing files being put through to committee without the actual primary source

Conclusion: Manual entry comment would need to state that the corrective actions were unsuccessful in eliminating additional inappropriate documentation or updates.

Qualitative Analysis on Reaudit, if applicable:
Enter N/A, if no additional finding during reaudit.

NCQA requires a qualitative analysis if any additional non-compliant documentation or updates were identified under the reaudit. Statement would need to include a description of the is
(Example: Licensure: *Issue Identified)*, and proposed corrective action statement and timeframes.

The corrective actions implemented have not been as effective in preventing inappropriate documentation or updates to the credentialing information based on follow-up audit and assessment. There was on additional incidences of inappropriate documentation and updates made to the credentialing application/ attestation.
Description: Another credentialing staff member updated the practitioner's attestation date without the practitioner resigning and dating the attestation.
Proposed corrective actions to include: Will complete additional one on one education with the specific staff member on the CII policies and NCQA's documentation requirements to be completed by 7/1/2025 by the Credentialing Director, and continue to monitor the automated process for resending of attestation to practitioner 60 days before expiration.

Qualitative Analysis: Manual entry to include the issue, proposed action plan and timeframes based on the reaudit findings.

Overall Effectiveness-Conclusion:

NCQA requires an overall statement to confirm effectiveness of correction actions implemented. See note in cell A50 and complete your summary conclusion in the box.

The corrective actions implemented have not been as effective in preventing inappropriate documentation or updates to the credentialing information based on follow-up audit and assessment. There was on additional incidences of inappropriate documentation and up ade to the credentialing application/ attestation and corrective actions as outlined above will continue to take place.

Overall effectiveness: Conclusion of overall actions that were put into place and results of the reaudit.

STOP! CII audit and Reaudit complete! Next audit due 12 months from the annual CII audit

Review of UVMHN C&E Policy 101 Credentialing System Controls, Access & Credentialing Information Integrity

1. Specialist must read the policy, prior to the training each year.
2. Specialist are encouraged to ask any questions about the policy during the training.

UVMHN C&E Supervisor or Director will audit staff documentation and updates into Credentialing Software system, at least yearly.
The credentialing software program maintains historical change data tracking to identify who has accessed the system, when and what actions were taken. The system provides reports on demand. The Credentialing & Enrollment Director or Supervisor generates and reviews activity reports.
Modifications to documentation and information listed below are deemed inappropriate

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

Corrective Action

1. The following corrective action will take place for inappropriate modification of data. The UVM Medical Center reserves the right to exercise corrective action it deems appropriate given the circumstance.
   1.1. Credentialing Specialist will be required to review Policy 101
   1.2. The Supervisor or Director will go over the modification(s) of data with the specialist. Upon review of the details the Supervisor or Director will make a determination if the modification(s) were completed in error or due to malintent.
      1.2.1. If the determination is made that the modification(s) were completed in error:
         1.2.1.1. The Credentialing Specialist will be provided with education and training.
         1.2.1.2. The Supervisor or Director will run Monthly reports for 3 consecutive months to monitor for inappropriate modifications and discuss with specialist as necessary.
            1.2.1.2.1. If additional inappropriate modifications are still being made after 3 consecutive months, Supervisor or Director will take corrective action, up to and including termination, in accordance with the UVMHN Corrective Action Policy.
      1.2.2. If the determination is made that the modification(s) were intentional:
         1.2.2.1. This activity will be addressed by corrective action, up to and including termination, in accordance with the UVMHN Corrective Action Policy.

2. In cases of a breach of confidentiality or if there is reason to believe that information has been shared in violation of this policy, the Director or Supervisor of Credentialing & Enrollment will request the relevant report(s). Appropriate actions will then be taken, up to and including termination, in accordance with the UVMHN Corrective Action policy.
3. Identified inappropriate access will be addressed by corrective action, up to and including termination, in accordance with the UVMHN Corrective Action policy.

Important Note – UVM Health Network C&E Staff are subject to compliance with UVMMC/UVMHN policies, as applicable. UVMHN C&E staff are employees of UVM Medical Center. The C&E operates as a department of UVM Health Network. UVMHN C&E's software contract is held by the UVMHN.

UVMHN C&E will document and report inappropriate documentation and updates to:

1. The organizations designated individual (s)
2. NCQA, when the organization identifies fraud and misconduct.

Training has been completed on (insert Date)
Training has been completed with (insert specialist name)
Training has been completed by (insert supervisor or Director name)

I acknowledge that I have read Policy 101 Credentialing System Controls, Access & Credentialing Information Integrity and this training document. I understand it is my responsibility to adhere to this policy. I have no further questions at this time, however, understand that I also have the responsibility to seek clarification from the Director or Supervisor of UVMHN C&E should questions regarding this policy and/or proper documentation standards in the future.

Signature of Trainee_____

Signature of Trainer_____