UCSF Benioff Children's Physicians Credentialing System Controls Policy & Oversight Procedure
Office of Origin: UCSF Office of Medical Affairs and Governance (OMAG)

I. PURPOSE

The purpose of this policy is to maintain compliance with the National Committee for Quality Assurance (NCQA) standards, particularly the CR1 credentialing policies pertaining to Elements C and D for credentialing system controls.

II. REFERENCES

National Committee for Quality Assurance (NCQA)

CR1 Element C – Credentialing System Controls

The organization's credentialing process describes:

1. How primary source verification information is received, dated, and stored.
    - The organization's policies and procedures describe how credentialing information is received, stored, reviewed, tracked, and dated.
2. How modified information is tracked and dated from its initial verification.
    - The organization's policies and procedures describe how it tracks modifications made to credentialing information:
        - When the information was modified.
        - How the information was modified.
        - Staff who made the modification.
        - Why the information was modified.
3. Staff who are authorized to review, modify, and delete information, and circumstances when modification or deletion is appropriate.
    - The organization's policies and procedures identify:
        - The level of staff who are authorized to access, modify, and delete information.
        - The circumstances when modification or deletion of information is appropriate.
4. The security controls in place to protect the information from unauthorized modification.
    - The organization's policies and procedures describe the process for:
        - Limiting physical access to credentialing information, to protect the accuracy of information gathered from primary sources and NCQA-approved sources.
        - Preventing unauthorized access, changes to and release of credentialing information.
        - Password-protecting electronic systems, including user requirements to:
            - Use strong passwords.
            - Avoid writing down passwords.
            - Create user IDs and passwords unique to each user.
            - Change passwords when requested by staff or if passwords are compromised.
5. How the organization audits the processes and procedures in factors 1-4.
    - The policies and procedures describe the organization's audit process for identifying and assessing risks and ensuring that specified policies and procedures are followed. At a minimum, the description includes:
        - The audit methodology used, including sampling, the individuals involved in the audit and the audit frequency.
        - Oversight of the department responsible for the audit.

CR1 Element D – Credentialing System Controls Oversight

1. Identify all modifications to credentialing and recredentialing information that did not meet the organization's policies and procedures for modifications as described in CR 1 - Element C, Credentialing System Controls.
2. Document and analyze all modifications that did not meet standards by doing a qualitative and quantitative analysis of all modifications.
3. Act on all findings. (Not applicable if no findings above.)

University of California, San Francisco (UCSF)

UCSF Identity and System Location Management System – Policy 650-10:
- http://policies.ucsf.edu/policy/650-10

UCSF Information Security and Confidentiality – Policy 650-16:
- http://policies.ucsf.edu/policy/650-16

UCSF Information Security and Confidentiality – Policy 650-16, Addendum A, UCSF Roles and Responsibilities for Securing Institutional Information and IT Resources:
- https://it.ucsf.edu/standard-guideline/ucsf-650-16-addendum-ucsf-roles-and-responsibilities-securing-institutional

UCSF Information Security and Confidentiality – Policy 650-16, Addendum B, UCSF Minimum Security Standards for Electronic Information Resources:
- https://it.ucsf.edu/standard-guideline/ucsf-650-16-addendum-b-ucsf-minimum-security-standards-electronic-information

UCSF Information Security and Confidentiality – Policy 650-16, Addendum F, UCSF Data Classification Standard:
- https://it.ucsf.edu/standard-guideline/ucsf-policy-650-16-addendum-f-ucsf-data-classification-standard

UCSF Information Technology Security Policy/Standards Hierarchy:
- https://it.ucsf.edu/ucsf-it-security-policystandards-hierarchy

UCSF Office of Health Compliance and Privacy Policy List:
- https://ohcp.ucsf.edu/ucsf-campus-policies-and-procedures

Unified UCSF Enterprise Password Standard
- See Addendum A

University of California Office of the President (UCOP)

University of California Electronic Information Security – Policy BFB-IS-3:
- https://policy.ucop.edu/doc/7000543/BFB-IS-3

University of California Electronic Communications Policy:
- https://policy.ucop.edu/doc/7000470/ElectronicCommunications

University of California UC Account and Authentication Management Standard:
- https://security.ucop.edu/files/documents/policies/account-and-authentication-management-standard.pdf

University of California Systemwide Information Security Tips and Fact Sheets Information:
- https://security.ucop.edu/resources/factsheets.html

University of California Information Technology Accessibility – Policy IMT-1300:
- https://policy.ucop.edu/doc/7000611/IMT-1300

University of California Information Technology Services Policies and Guidelines Index:
- https://www.ucop.edu/information-technology-services/policies/index.html

III. PROCEDURE

CR1 C – Factor 1: Primary Source Verification Information How credentialing information is received, stored, reviewed, tracked, and dated.	
How primary source verification is received.	All providers are instructed to submit their initial and recredentialing applications online, along with any supplemental documents, through the UCSF credentialing portal titled UC Me. Once submitted, the Credentials Verification Organization (CVO) Program Manager will assign the initial or recredentialing application to a CVO analyst for assessment and review via the Echo credentialing database and an internal UCSF credentialing platform known as TaskMaster. The Echo credentialing database stores all credentialing information, while the TaskMaster credentialing platform is utilized as an electronic credentialing checklist for initial and recredentialing files. Primary source verifications are received by CVO analysts as a part of their assessment and review, and may be re-reviewed by CVO auditors for quality assurance. Primary source verifications can be received by the following methods: • Internet Websites: At UCSF, primary source verifications are mostly obtained online via internet websites. Primary source verifications obtained via internet websites will exhibit the name of the issuing source (i.e., organization, institution, etc), name of provider who is being verified, type of verification (i.e., license, education, board certification, etc), along with issuance and expiration dates as applicable. • E-mail: Primary source verifications may be received via e-mail if supplied directly by the issuing source. Primary source verifications received via e-mail will show the name of the issuing source (i.e., organization, institution, etc), name of the provider who is

	being verified, type of verification (i.e., license, education, board certification, etc), along with issuance and expiration dates as applicable. • Digital Fax: Primary source verification may be received via digital fax if provided directly by the issuing source. At UCSF, digital faxes are electronically routed and delivered to the appropriate CVO analyst. Primary source verifications received via digital fax will identify the name of the issuing source (i.e., organization, institution, etc), name of the provider who is being verified, type of verification (i.e., license, education, board certification, etc), along with issuance and expiration dates as applicable. • Verbal: Primary source verification may be verbally received via telephone if provided directly by the issuing source. The CVO analyst will document the name of the issuing source (i.e., organization, institution, etc) and staff who they spoke with, name of the provider who is being verified, type of verification (i.e., license, education, board certification, etc), date of telephone call, and issuance and expiration dates as applicable. • Mail: Primary source verification may be mailed by the issuing source via the United States Postal Service, FedEx, United Parcel Service, and/or other delivery services. Such mail is delivered to the UCSF OMAG office and received by the appropriate CVO analyst. Primary source verifications received via mail will identify the name of the issuing source (i.e., organization, institution, etc), name of the provider who is being verified, type of verification (i.e., license, education, board certification, etc), along with issuance and expiration dates as applicable. Physical copies of primary source verifications received via mail are shredded and destroyed once they have been scanned and uploaded into the Echo credentialing database. The receipt date of primary source verification is consistent with NCQA requirements. Primary source verifications are automatically date-stamped when received to ensure of compliance with the 180-day time limit from the UCSF Credentials Committee meeting date. The receipt date for electronic primary source verifications is the date that the CVO analyst verified a provider's credentials, while the receipt date for written primary source verifications is the date listed on the letter. If attempts to obtain and receive primary source verification are unsuccessful, secondary source verification may be utilized instead. Secondary source verification is defined as the verification of a provider's credentials based upon evidence obtained by methods other than directly from the issuing source of the provider's credentials.
How primary source verification is stored.	All electronic credentialing files, including any applicable primary source verifications, are securely stored within the Echo credentialing database. After a CVO analyst completes their assessment and review of an initial or recredentialing application via the TaskMaster credentialing platform, an electronic credentialing file known as a Provider Assessment Portal (PAP) packet is generated within the Echo credentialing database. The PAP packet combines the entirety of a provider's initial or recredentialing application, supplemental documents, and primary source verifications into an electronic credentialing file. Storage protocols for primary storage verifications include: • Initial and recredentialing applications are stored in the UC Me credentialing portal via a secure server. The UC Me credentialing portal is managed by the Credentialing Database Administrator and UCSF Information Technology (IT) Department. • All primary source verifications are stored in the Echo credentialing database via a secure server. The Echo credentialing database is managed by the Credentialing Database Administrator and UCSF IT Department. • Physical copies of credentialing information, including primary source verifications received via mail, are kept in locked file cabinets at the UCSF OMAG office until they can be scanned and uploaded in the Echo credentialing database. Once scanned and uploaded, physical copies of primary source verifications are immediately shredded and destroyed.
How primary source verification is reviewed.	When a provider submits their initial or recredentialing application, primary source verifications are obtained, received, and uploaded by CVO analysts as a part of their assessment. Primary source verifications are subsequently reviewed by CVO auditors for quality assurance prior to an initial or recredentialing file being presented for final recommendation by the UBCP

	Credentials Committee. All primary source verifications are automatically date-stamped when obtained, received, and uploaded.
How primary source verification is tracked.	Primary source verification is tracked during providers' initial and recredentialing processes, as well as on a regular basis for all expirable credentials. In the latter, the tracking of expirable credentials refers to ongoing monitoring between recredentialing cycles, and entails the review of adverse information, limitations, and sanctions as applicable. When a primary source verification has been obtained and received, it is uploaded and saved into the Echo credentialing database by a CVO analyst. Within the Echo credentialing database, the following information is captured within a provider's credentialing record to track the primary source verification, including: • Verification type (i.e., license, education, insurance, etc) • Issuing source (i.e., organization, institution, etc) • Number or identifier pertaining to provider's credentials • Issuance date • Renewal date • Expiration date • Receipt date • Review date Any modifications made to primary source verifications within the Echo credentialing database are automatically tracked by the CVO analyst's username, along with the date and time that the modification was made. The automatic tracking of a CVO analyst's username, along with the date and time that the modification was made cannot be altered.
How primary source verification is dated.	All primary source verifications obtained and saved into the Echo credentialing database and TaskMaster credentialing platform are automatically date-stamped with the username of the CVO analyst who uploaded such primary source verification.

CR1 C – Factor 2: Tracking Modifications How modifications to credentialing information are tracked.	
When the information was modified.	Any modifications made to credentialing information within the Echo credentialing database are automatically tracked by the UCSF OMAG staff member's username, in addition to the date and time that the modification was made. Information received directly via primary source verification cannot be modified, unless clarifying information has been obtained. In such situation, the clarifying information is uploaded as supplemental documentation within the Echo credentialing database. All modifications are automatically tracked in an audit trail log, which can be pulled by the Credentialing Database Administrator as required.
How the information was modified.	Modifications of credentialing information within the Echo credentialing database comprise of 3 types: 1. Additions: Adding credentialing information 2. Changes: Changing credentialing information 3. Deletions: Deleting credentialing information Within an audit trail log, modifications are automatically tracked and identified by type. Example: If a provider submits a new board certification, such board certification would be verified via primary source and uploaded into the provider's credentialing record within the Echo credentialing database. Appropriately, an audit trail log would display the UCSF OMAG staff member's username, date, time, and type of modification that was made within the Echo credentialing database.
Staff who made the modification.	All UCSF OMAG staff are assigned an unique username in order to access the Echo credentialing database. The unique username is associated with each UCSF OMAG staff member's computer and e-mail accounts as established by the UCSF IT Department via single sign-on (SSO). SSO is a method which permits access to computer applications, e-mail accounts, and websites through a single set of credentials (username and password). SSO works in concurrence with multi-factor authentication, which necessitates multiple identifying factors before UCSF OMAG staff are allowed access to computer applications, e-mail accounts, and websites. Correspondingly, when modifications are made to credentialing information within the Echo credentialing database, the Echo username of the UCSF OMAG staff member is automatically tracked, along with the date and time.

Why the information as modified.	If a modification is made to credentialing information within the Echo credentialing database, UCSF OMAG staff must upload the supplemental documentation to justify why such modification was made. Such supplemental documentation may include primary source verification and/or an e-mail directly from a provider that explains the reason for the modification. Moreover, UCSF OMAG staff will enter a comment within the credentialing record to detail what modification was made along with their initials and date. Example: If a provider's submits a copy of their renewed malpractice insurance certificate, the UCSF OMAG staff member will update the applicable data fields, upload the renewed malpractice insurance certificate, and enter a comment within the credentialing record to detail what modification was made with their initials and date ("Reviewed and updated malpractice insurance certificate. 11/1/2022 EC"). Modifications saved within the Echo credentialing database automatically track the UCSF OMAG staff member's username, date, and time.

CR1 C – Factor 3: Authorization to Modify Information
The level of staff who are authorized to access, modify, and delete information, and the circumstances when modification or deletion of information is appropriate.

Level of staff who are authorized to access, modify, and delete information.

The level of access to credentialing information within the Echo credentialing database for all UCSF OMAG staff is determined by the hiring manager and administered following the completion of the onboarding process. All UCSF OMAG staff are granted an unique Echo username in conjunction with their computer and e-mail accounts as established by the UCSF IT Department via single sign-on (SSO). SSO is a method which permits access to computer applications, e-mail accounts, and websites through a single set of credentials (username and password). After an UCSF OMAG staff member's computer and e-mail accounts have been created, the hiring manager will send an e-mail request to the UCSF IT Departmental Applications Manager and specify the level of access within the Echo credentialing database to be granted.

All UCSF OMAG staff are assigned to 1 of 5 security groups based on their job titles and roles. Each security group permits explicit levels of access to credentialing information within the Echo credentialing database.

Security Group	UCSF OMAG Job Title and Role
Echo Security (full system access)	Credentialing Database Administrator
Administrator (access to create and schedule recurring reports, plus Manager and Medical Staff Team security group abilities)	Vice President of Medical Staff Governance
Manager (access to privilege form maintenance and audit trail log, plus Medical Staff Team security group abilities)	Credentialing and Privileging Director
Medical Staff Team (access to view, add, change, and delete credentialing information)	<u>Supervisors</u> Credentialing Process Improvement (CPI) Program Manager, CVO Program Manager, Health Plan Enrollment (HPE) Director, Strategic Initiatives Unit (SIU) Director <u>Auditors</u> CVO Auditors <u>Analysts</u> CPI Analysts, CVO Analysts, HPE Analysts, SIU Analysts
Read Only (access to view credentialing information only)	Finance and Operations Manager

On a monthly basis, the Credentialing and Privileging Director and/or designee will review an automatically-generated report that showcases the authorized UCSF OMAG staff with access to the Echo credentialing database and their assigned security groups. If determined that an

	UCSF OMAG staff member no longer requires access to the Echo credentialing database, an e-mail request will be sent to the UCSF IT Department to terminate such access. UBCP credentialing staff cannot access the Echo credentialing database. Rather, UBCP credentialing staff may only view initial and recredentialing files when granted a direct link to completed Provider Assessment Portal (PAP) packets. PAP packets are generated as a part of review and assessment that is conducted by UCSF OMAG staff and combine the entirety of a provider's initial or recredentialing application, supplemental documents, and primary source verifications. PAP packets are delivered via portable document format (PDF) and cannot be modified.
Circumstances when modification or deletion of information is appropriate.	Appropriate circumstances of when modification or deletion of credentialing information within the Echo credentialing database include: • Updates to demographic information • Updates to clinical and administrative addresses • Updates to telephone and fax numbers • Updates to education and/or post-graduate training • Updates to work history • Updates to licenses and certifications • Updates to staff statuses • Correction of data entry errors • Deletion of duplicative credentialing information • Deletion of credentialing information if uploaded to incorrect provider's credentialing record Inappropriate circumstances of when modification or deletion of credentialing information within the Echo credentialing database include: • Alteration of staff status and credentialing approval dates that were not approved by the UBCP Credentials Committee • Alteration of primary and secondary source verification dates • Alteration of supplemental documentation of credentialing information • Alteration of signatures and dates on electronic and/or physical credentialing documents • Unauthorized deletion of credentialing information All modifications and deletions of credentialing information within the Echo credentialing database are automatically tracked by the UCSF OMAG staff member's username, along with the date and time that the modification or deletion was made—which can be pulled by the Credentialing Database Administrator as required. Supplemental documentation must be uploaded when modification or deletion of credentialing information occurs within the Echo credentialing database for justification purposes.

CR1 C – Factor 4: Securing Information Limiting physical access to credentialing information; preventing unauthorized access, changes to, and release of credentialing information; password-protecting electronic systems; and disabling or removing passwords of employees who leave the organization and alerting appropriate staff who oversee computer security.	
Limiting physical access to credentialing information, to protect the accuracy of information gathered from primary sources and NCQA-approved sources.	The UCSF credentialing process is entirely electronic. The secure server which stores the Echo credentialing database, TaskMaster credentialing platform, and UC Me credentialing portal is located at an UCSF data center in an undisclosed location separate from the UCSF OMAG office. Only UCSF IT Department staff members may physically access the secure server. To electronically access credentialing information within the Echo credentialing database, TaskMaster credentialing platform, and UC Me credentialing portal, UCSF OMAG staff must be remotely connected to the UCSF virtual private network (VPN) via single sign-on (SSO). SSO is a method which permits access to computer applications, e-mail accounts, and websites through a single set of credentials (username and password). SSO requires the utilization of multi-factor authentication, which necessitates multiple identifying factors before UCSF OMAG staff are allowed access to computer applications, e-mail accounts, and websites, such as the Echo credentialing database, via the UCSF VPN. Accordingly, when modifications are made to

	credentialing information within the Echo credentialing database, the Echo username of the UCSF OMAG staff member is automatically tracked, in addition to the date and time. All physical copies of credentialing information (i.e., old credentialing files) must be stored out of sight and kept in locked file cabinets within the UCSF OMAG office when not in use. Credentialing documents received via mail (i.e., primary source verification) are also kept in locked file cabinets within the UCSF OMAG office until they can be scanned and uploaded in the Echo credentialing database. Once scanned and uploaded, physical copies of primary source verifications are immediately shredded and destroyed. To physically access the UCSF OMAG office, all UCSF OMAG staff are required to swipe their identification badge at a badge reader, which is located at all main points of entry (i.e., doors, hallways, etc). The swiping of identification badges allows UCSF Security Services to track all UCSF staff at any given location with dates and times. Identification badges include each UCSF staff member's picture, full name, credentials (if any), department, and job title. Physical access to buildings and/or facilities must be requested by an UCSF staff member's manager and approved by UCSF Security Services before conferred.
Preventing unauthorized access, changes to, and release of credentialing information.	Only authorized UCSF OMAG staff may access to credentialing information within the Echo credentialing database. The UCSF OMAG management team works with the UCSF IT Department to ensure explicit levels of access have been appropriately granted to UCSF OMAG staff via assigned security groups. UCSF OMAG staff must be remotely connected to the UCSF virtual private network via single sign-on and have completed multi-factor authentication to log into the Echo credentialing database. Providers and non-UCSF OMAG staff (including UBCP credentialing staff) cannot access or view any credentialing information within the Echo credentialing database. Any modifications made to credentialing information within the Echo credentialing database are automatically tracked by the UCSF OMAG staff member's username, along with the date and time that the modification was made. All modifications are automatically tracked within an audit trail log, which can be pulled by the Credentialing Database Administrator as required. UCSF OMAG staff members are mandated to annually attest to the UCSF Code of Conduct and complete an online cybersecurity awareness training, which set the confidentiality and privacy principles that UCSF OMAG staff members must abide by. Credentialing information may only be released if a requestor presents a signed information release form from the provider. A signed information release form must contain the provider's full name, signature, and date from within the past 180 days to be valid. Only credentialing information that is requested will be released. Any inquiries from legal attorneys and/or malpractice insurance companies will be forwarded to the UCSF Risk Management Department. Credentialing file audits performed by third-party entities (e.g., health plans, payors, etc) must conducted in accordance with the following guidelines: • Credentialing file audits must be scheduled in advance on a date and time that is mutually established by UBCP, UCSF OMAG, and the third-party entity. • Auditors from the third-party entity must sign a confidentiality agreement. • Auditors from the third-party entity cannot photocopy, remove, or disseminate any credentialing information. • The UCSF OMAG management team and/or designee will provide direct supervision of a credentialing file audit to ensure no credentialing information is accessed without authorization. Any unauthorized access, modifications, or release of credentialing information may result in disciplinary action or immediate termination of UCSF OMAG staff.
Password-protecting electronic systems, including user requirements to:	All UCSF OMAG staff are assigned an unique username in order to access the Echo credentialing database, TaskMaster credentialing platform, and UC Me credentialing portal. The unique username is associated with each UCSF OMAG staff member's computer and e-mail accounts as established by the UCSF IT Department via single sign-on (SSO). SSO is a method which permits access to computer applications, e-mail accounts, and websites through

-Use strong passwords. -Avoid writing down passwords. -Create user IDs and passwords unique to each user. -Change passwords when requested by staff or if passwords are compromised.	a single set of credentials (username and password). SSO works in concurrence with multi-factor authentication, which necessitates multiple identifying factors before UCSF OMAG staff are allowed access to computer applications, e-mail accounts, and websites. For new UCSF OMAG staff, a default password is provided by the UCSF IT Department. New UCSF OMAG staff must create a new password upon their first log-in. The Unified UCSF Enterprise Password Standard (see Addendum A) was approved by the UCSF Chief Information Officer on October 1, 2010 and is applicable to all UCSF staff for access to password-protected systems such as the Echo credentialing database, TaskMaster credentialing platform, and UC Me credentialing portal. The Unified UCSF Enterprise Password Standard solicits the use of strong passwords with: • Minimum password length of 12 characters • Maximum consecutive character repeat of 2 characters • 3 out of 4 characters must consist of upper/lower case, numbers, symbols • Prohibition of easily guessed patterns like dates, telephone numbers, proper names, minor variations on former password UCSF staff may manage and change passwords via the UCSF Password Management Tool website (https://password.ucsf.edu/prod/). UCSF computer and e-mail accounts that have been compromised will be automatically locked, in which UCSF staff will also be directed to the UCSF Password Management Tool website to change passwords. Respectively, all UCSF staff are mandated to annually attest to the UCSF Code of Conduct, which requires compliance with password safekeeping principles, including not writing them down. UCSF enforces an annual password change policy that requires all UCSF staff to change their password at least once a year. All UCSF staff are prompted by an automated password change script within 12 months from the date that their password was last changed. The automated script is a part of a password auditing software referred to as Active Directory (AD) Audit Plus via ManageEngine that is managed by the UCSF IT Department. If an UCSF staff member fails to change their password annually, access to computer applications, e-mail accounts, and websites will be automatically disabled. Passwords for all UCSF computer applications, e-mail accounts, and websites, including the Echo credentialing database, TaskMaster credentialing platform, and UC Me credentialing portal, are always masked as a protective measure. Masked passwords are obscure representations of actual passwords via asterisks, bullet points, and/or other symbols.
Disabling or removing passwords of employees who leave the organization and alerting appropriate staff who oversee computer security.	Upon the resignation or termination of UCSF OMAG staff, managers will submit an Account Request Form to the UCSF IT Department to terminate all access to UCSF computer and e-mail accounts, including the Echo credentialing database, TaskMaster credentialing platform, and UC Me credentialing portal. This process also includes the immediate disabling of UCSF OMAG staff credentials (username and password).

CR1 C – Factor 5: Credentialing Process Audit The audit process for identifying and assessing risks and ensuring that specified policies and procedures are followed. At a minimum, the description includes the audit methodology used, including sampling, the individuals involved in the audit and the audit frequency; and oversight of the department responsible for the audit.	
Audit methodology used, including sampling, the individuals involved in the audit and the audit frequency.	CR1 C – Factor 1: Primary Source Verification Information All (100%) UBCP initial and recredentialing files are subjected to audit by CVO auditors for quality assurance. CVO auditors will review the entirety of a credentialing file, including accuracy and completeness of the initial or recredentialing application, primary source verifications, supplemental documentation, and data entry within the Echo credentialing database. In particular, CVO auditors will review primary source verifications for validity of: • Verification type (i.e., license, education, etc) • Issuing source (i.e., organization, institution, etc) • Number or identifier pertaining to provider's credentials • Issuance date • Renewal date

- Expiration date
- Receipt date
- Review date

If deemed non-compliant, a credentialing file will be returned to the assigned CVO analyst for follow-up. CVO auditors' commentary and feedback are documented within the TaskMaster credentialing platform, which is programmed to automatically generate weekly CVO analyst reports as a part of the UCSF OMAG quality improvement infrastructure. Such reports gauge each CVO analyst's quality and productivity by offering qualitative and quantitative feedback. The qualitative feedback encompasses CVO auditors' commentary and feedback on how CVO analysts should improve their performance, while the qualitative feedback depicts the total number of credentialing files that was completed without any issues versus the total number of credentialing files that was returned for follow-up. Weekly CVO analyst reports are e-mailed to each CVO analyst on the following Monday with their performance data from the prior week.

After initial and recredentialing files have been deemed compliant by CVO auditors, UBCP credentialing staff will re-audit all (100%) initial and recredentialing files prior to presenting them for final recommendation to the UBCP Credentials Committee as a secondary form of quality assurance. UBCP credentialing staff may only view initial and recredentialing files when granted a direct link to completed Provider Assessment Portal (PAP) packets. PAP packets are generated as a part of review and assessment that is conducted by UCSF OMAG staff, and combine the entirety of a provider's initial or recredentialing application, supplemental documents, and primary source verifications. PAP packets are delivered via portable document format (PDF) and cannot be modified.

<u>CR1 C – Factor 2: Tracking Modifications</u>
Any modifications (additions, changes, deletions) made to credentialing information within the Echo credentialing database are automatically tracked within an audit trail log, which is organized by the UCSF OMAG staff member's username, modification type, and the date and time that the modification was made. On a monthly basis, an audit trail report will be automatically delivered by the UCSF IT Department via e-mail to the Credentialing and Privileging Director and/or designee. The audit trail report compiles data from the audit trail log and delineates a total of 50 randomly-selected active credentialing records in which modifications have been made to credentialing information within those records. Once delivered, the Credentialing and Privileging Director and/or designee will audit report findings to determine compliance of each modification to UCSF OMAG departmental standards. If a modification is deemed non-compliant, the report finding will be documented, and the UCSF OMAG staff member who made such modification will be educated to prevent the recurrence of such errors. Disciplinary action, immediate termination, and/or revocation of access to the Echo credentialing database may occur if such modification error is repeated by the same UCSF OMAG staff member. The audit trail report may also be manually pulled from the UCSF IT Department if requested by the Credentialing and Privileging Director, designee, and/or UCSF OMAG management team.

<u>CR1 C – Factor 3: Authorization to Modify Information</u>
The level of access to credentialing information within the Echo credentialing database for all UCSF OMAG staff is authorized by the hiring manager and administered following the completion of the onboarding process. On a monthly basis, an Echo users report will be automatically delivered by the UCSF IT Department via e-mail to the Credentialing and Privileging Director and/or designee. The Echo users report showcases the authorized UCSF OMAG staff with access to the Echo credentialing database and their assigned security groups. The Credentialing and Privileging Director and/or designee will audit the Echo users report to determine whether all authorized UCSF OMAG staff have been granted appropriate levels of access to the Echo credentialing database based on their assigned security groups in relation to their job titles and roles. An e-mail request will be sent to the UCSF IT Department to terminate access to the Echo credentialing database for UCSF OMAG staff who no longer require it. The Echo users report may also be manually pulled from the UCSF IT Department if requested by the Credentialing and Privileging Director, designee, and/or UCSF OMAG management team.

	CR1 C – Factor 4: Security Information All credentialing systems at UCSF OMAG are password-protected, including the Echo credentialing database, TaskMaster credentialing platform, and UC Me credentialing portal. UCSF enforces an annual password change policy. Annual password changes must be done in accordance with the Unified UCSF Enterprise Password Standard (see Addendum A). All UCSF staff are prompted by an automated password change script within 12 months from the date that a password was last changed. The automated script is a part of a password auditing software that is managed by the UCSF IT Department. If an UCSF staff member fails to change their password annually, access to computer applications, e-mail accounts, and websites will be automatically disabled. On a monthly basis, a password report is compiled and delivered via e-mail from the UCSF IT Department to the Credentialing and Privileging Director and/or designee. The password report identifies UCSF OMAG staff's compliance data for the following measures: • Date that password was last changed • Compliance with UCSF annual password change policy The Credentialing and Privileging Director and/or designee will review the password report to ensure that all UCSF OMAG staff are compliant with the annual password change policy. Any suspicion of inappropriate access to credentialing information may result in investigation and disciplinary action in accordance with UCSF Human Resources policies. Investigations may include, but are not limited to: • Auditing of access to UCSF computer applications and websites • Physical inspection of UCSF computer equipment and devices
Oversight of the department responsible for the audit.	Oversight of UCSF OMAG is governed by the UBCP Credentials Committee and other medical staff leadership, including the UCSF Chancellor, UCSF Governance Advisory Council, UCSF Executive Medical Board, and UCSF Credentials Committee. Oversight of the UCSF IT Department is governed by the UCSF Chief Information Officer, UCSF Chief Executive Officer, University of California Office of the President, and University of California Board of Regents.

CR1 D – Credentialing System Controls Oversight Identify all modifications to credentialing and recredentialing information that did not meet the organization's policies and procedures for modifications as described in CR 1 - Element C, Credentialing System Controls; document and analyze all modifications that did not meet standards by doing a qualitative and quantitative analysis of all modifications; and act on all findings (not applicable if no findings above.)	
Identify all modifications to credentialing and recredentialing information that did not meet the organization's policies and procedures for modifications as described in CR 1 - Element C, Credentialing System Controls.	Resultant of the auditing processes established within the "CR1 C – Factor 5: Credentialing Process Audit" section, any modifications to credentialing and recredentialing information that do not meet the UCSF OMAG departmental standards will be identified and documented. The oversight of such modifications will be completed at least annually and will be incumbent upon the automated audit trail reports that are sent to the Credentialing and Privileging Director, designee, and/or UCSF OMAG management team from the UCSF IT Department every month. Inappropriate modifications will be recorded within the Monitoring and Reporting of Inappropriate Modifications Report.
Document and analyze all modifications that did not meet standards by doing a qualitative and quantitative analysis of all modifications.	Qualitative Analysis The Credentialing and Privileging Director, designee, and/or UCSF OMAG management team will review any identified modifications to credentialing and recredentialing information that do not meet the UCSF OMAG departmental standards and perform root cause analyses. Root cause analyses will entail addressing deficiencies and/or revising processes that are creating barriers to improvement or causing additional failures. Once root cause analyses have been completed, the Credentialing and Privileging Director and/or UCSF OMAG management team will meet with the appropriate UCSF OMAG staff to implement corrective actions.

	Quantitative Analysis: When 3 or more inappropriate modifications of the same theme have been made to credentialing and recredentialing information, the Credentialing and Privileging Director and/or designee will escalate such issue to the UCSF OMAG management team to be immediately addressed. Corrective actions here may include educating and informing UCSF OMAG staff and/or instilling parameters within the Echo credentialing database to automatically deny such inappropriate modifications from being made. Written documentation, including updating the UCSF Medical Staff Organization Credentialing Policy and Procedure, may also arise to deter further instances of such inappropriate modifications. Disciplinary action or revocation of access to the Echo credentialing database may be taken if inappropriate modifications persist.
Act on all findings. (Not applicable if no findings above.)	Any corrective actions taken based upon inappropriate modifications to credentialing and recredentialing information will be documented within the Monitoring and Reporting of Inappropriate Modifications Report. The UCSF OMAG management team will meet on a quarterly basis to review any corrective actions that have been taken to assess their effectiveness. Ongoing monitoring will continue until improvements have been demonstrated for at least 3 consecutive quarters.

IV. RESPONSIBILITY

All questions concerning this policy may be directed to UCSF OMAG at (415) 885-7268.

V. HISTORY OF REVISIONS

- Revisions approved at June 2023 UBCP Credentials Committee
- Revisions approved at July 2022 UBCP Credentials Committee
- Revisions approved at January 2022 UBCP Credentials Committee
- Initial approval at June 2021 UBCP Credentials Committee

VI. ADDENDUM A

Unified UCSF Enterprise Password Standard

VII. ADDENDUM B

Credentialing System Controls Audit Report Template

Unified UCSF Enterprise Password Standard

Created by Esther Silver, last modified on Nov 09, 2018

Policy Type

Standard

This Unified UCSF Enterprise Password Standard was approved by the UCSF CIO on October 1, 2010, and is applicable to all Electronic Information Resources within UCSF, including the Medical Center. Questions about this standard can be sent to the Security & Policy Group, at security@ucsf.edu

Category	Standard
Failed logons allowed before lockout	5 failed attempts
Lockout duration	15 minutes
Minimum password length	12
Maximum consecutive character repeats	2
Required characters	At least one in 3 of 4 character sets: Upper/lower case, numbers, symbols
Prohibited patterns	Easily guessed patterns: dates, phone numbers, proper names, minor variations on former password

This standard should be considered a minimum. Systems that are capable of exceeding these standards should if operationally feasible.

Privileged administrator accounts with access to sensitive Windows systems should use passphrases that are 15 or more characters in length and meet the other requirements within this standard. Passphrases should be reset at least every 90 days.

Important Reminders

- Pick as strong a password as possible and keep it safe. If at any time, you feel your password may have been compromised, change it.
- Certain regulations may require password aging for specific systems. For example, Payment Card Industry Data Security Standard (PCI-DSS) requires password changes every 90 days. PCI system owners are responsible for the implementation of password aging and should NOT rely on the minimum standard.

Exceptions

All systems must comply with the password standard if possible. There are some cases in which an exception may be granted, including:

- Technical limitations
- Regulatory reasons

Systems granted an exception may be required to have additional compensating information security controls in place, such as a stricter firewall, or greater access logging.

Exception Process

All exception requests should be directed to the UCSF IT Service Desk: online at http://help.ucsf.edu/ or by phone (415) 514-4100.

UCSF Security & Policy (S&P) will investigate the request and render a decision. Requests will be reviewed by the Security and IT Policy Committee a periodic basis.

Exception Requests

Exception requests must contain the following information at a minimum:

- Name of the individual
- Affiliation/Title of the individual(s)
- Name of the system(s)
- Types of data the account(s) will have access to, particularly, any access to Restricted Information such as ePHI or PII
- Types of data on the system(s) where the exception(s) will be effective, particularly, any access to Restricted Information such as ePHI or PII
- Reason for the request
- Duration, e.g., temporary (with start and end times) or permanent

Granted Exceptions

Exceptions granted will be tracked by S&P and will be reviewed every 12 months to ensure exceptions are still valid and required

CREDENTIALING SYSTEM CONTROLS AUDIT REPORT

National Committee for Quality Assurance (NCQA) requires the Health Plan to monitor its delegates to ensure appropriate oversight of credentialing system security controls was completed, at least annually.

Instructions: Complete the information below with all applicable information. All sections must be completed. If you conduct audits more frequently than annually, the Credentialing System Controls Report should be a summary of the multiple audits that were conducted during the look back period.

Additional Evidence:

- If requested, you will be required to provide evidence of the audit(s) you conducted.
- If noncompliant modifications were identified: Complete the "***Noncompliant Modifications Report".***

Delegate Name:					
Delegate Person/ Title who conducted Audit:					
Date(s) of Audit completed:					
Time period of Audit:					
Audit included:	☐ Electronic Files		☐ Paper Files		☐ Both
Audit Frequency:	☐ Monthly	☐ Quarterly	☐ Semi-Annually	☐ Annually	☐ Other(explain)

TYPE(s) OF CREDENTIALING SYSTEM

Select the appropriate box(s) that applies to the type of credentialing system that your organization uses.

☐	1. Advanced system controls capabilities: Automatically records dates ***and*** prevents changes that do not meet the policy - *monitoring is not required.* **Note, if selected**: Your policy needs to describe how the functionality of the system ensures compliance and provide evidence or documentation of the advanced system control capabilities. (e.g., screen prints, etc).
OR	
☐	2. Credentialing System: Choose A, B, **or** C
☐	A. The credentialing system can identify **all noncompliant** modifications. (Sampling is **not** allowed and all noncompliant modifications must be reviewed)
☐	B. The credentialing system is **not able** to identify **any** modifications and/or paper files are used. (Sampling is allowed)
☐	C. The credentialing system can identify **all** modifications. (Sampling is allowed)

AUDIT METHODOLOGY

Sampling: The audit of 5% or 50 files (minimum of 10/10) must contain files **with** modifications. If the original file sample did not include files that contained modifications, you must continue to pull files from the entire universe in the look back period (since last audit) until the minimum sampling size of files **with modifications** has been reached. Those files with modifications are then reviewed to determine if the modifications made are compliant or noncompliant.

Modifications: Applies to credentialing information in elements CR 2 through CR 5.

This section must be completed to its entirety.

Total File Universe in look back period (initials + recredentialing files)	

Select the appropriate audit method used:

☐	**5% or 50 files (min of 10 initial cred /10 recred) methodology was utilized**			
		initial files reviewed with modifications		recred files reviewed with modifications
☐	**All files with modifications reviewed (no sampling utilized)**			
		Number of files reviewed with modifications		
☐	**Total file universe reviewed, no files with modifications were identified**			

Number (#) or percent (%) of Files with modifications that **did not meet** your criteria:	

- If noncompliant modifications were identified: Complete the "***Noncompliant Modifications Report"*** report.

CREDENTIALING SYSTEM CONTROLS AUDIT RESULTS

☐ An audit of all modifications to the credentialing system/files has been completed and all the modifications were deemed compliant based off our policies, procedures, and delegation agreement.

☐ An audit was completed of the entire universe and no modifications were identified based off our policies, procedures, and delegation agreement

☐ An audit of all modifications to the credentialing system/files has been completed and **noncompliant** modifications were identified based off our policies, procedures, and delegation agreement. ***The report of all noncompliant modifications is attached.***

Name: _____ **Date:** _____

Signature of Person Completing the Report: _____

I attest the above information is truthful, accurate and complete to the best of my ability