Office of Medical Affairs and Governance (OMAG)
Credentialing System Controls Policy & Oversight Procedure

Office of Origin: Medical Staff Services Office – (415) 885-7268

I. PURPOSE

The purpose of this policy is to maintain compliance with the National Committee for Quality Assurance (NCQA) standards, specifically CR1 Element C & D, Credentialing System Controls.

II. REFERENCE

NATIONAL COMMITTEE FOR QUALITY ASSURANCE (NCQA)

CR1 Element C – Credentialing System Controls

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.
   - Circumstances when modification or deletion 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.
     - Use different passwords for different accounts.
     - Change passwords periodically.
   - Changing or withdrawing passwords, including alerting appropriate staff who oversee computer security to:
     - Change passwords when appropriate.
     - Disable or remove passwords of employees who leave the organization.
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 elements include:
  - methodology used;
  - including sampling;
  - individuals involved in the audit; and
  - 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 organizations policies/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. Acting on all findings. (Not applicable if no findings above.)

UNIVERSITY OF CALIFORNIA SAN FRANCICO (UCSF)

Identity and System Location Management System

- http://policies.ucsf.edu/policy/650-10

Information Security and Confidentiality

- http://policies.ucsf.edu/policy/650-16
- Addendum B - Minimum Security Standards for Electronic Information Resources
  - https://it.ucsf.edu/standard-guideline/ucsf-650-16-addendum-b-ucsf-minimum-security-standards-electronic-information

IT Security Policy Standard Hierarchy

- https://it.ucsf.edu/ucsf-it-security-policystandards-hierarchy

Medical Center Policies & Procedures – Office of Healthcare Compliance and Privacy

- https://ohcp.ucsf.edu/ucsf-medical-center-policies-and-procedures
- Safeguarding the Privacy and Confidentiality of UCSF Information and Data
  - https://ucsfpolicies.ucsf.edu/Shared%20Documents/SafeguardingPrivacyConfiUCSFDataandInfo.pdf

Unified UCSF Enterprise Password Standard

- Attached Addendum A - https://wiki.library.ucsf.edu/x/8CQvGw

UNIVERSITY OF CALIFORNIA – OFFICE OF THE PRESIDENT

Identity and Access Management policy

- https://policy.ucop.edu/doc/7020450/BFB-IS-11

Electronic Communications Policy

- https://policy.ucop.edu/doc/7000470/ElectronicCommunications

Electronic Information Security Policy

- https://policy.ucop.edu/doc/7020450/BFB-IS-11

Electronic Information Security Policy FAQs

- https://security.ucop.edu/files/documents/policies/is-3-faq.pdf

Ethics, Compliance and Audit Services – HIPAA

- https://policy.ucop.edu/doc/7000470/ElectronicCommunications

Systemwide Information Security Factsheets

- https://security.ucop.edu/resources/factsheets.html#general

Systemwide IT Policies & Guidelines • https://www.ucop.edu/information-technology-services/policies/index.html **University California – Systemwide IT Policy Glossary** • https://www.ucop.edu/information-technology-services/policies/index.html

III. Procedure

CR 1.C.1 Primary Source Verification (CR1. Element C #1) How credentialing information is received, stored, reviewed, tracked, and dated.	
How applications, primary and secondary source verifications are received.	Credentialing applications and supporting documentation are received via our TaskMaster credentialing platform as submitted by applicants through our UC Me application portal. All primary source verifications (PSVs) collected as part of the UCSF credentialing for initial and reappointment applications are reviewed by an OMAG file auditor or manager. Files cannot move on to be reviewed by clinical leadership and our respective Credentials Committee/Interdisciplinary Committee membership without first being reviewed for all appropriate primary source verifications and deemed audit complete by our OMAG team. Primary source verifications are received or obtained by primary source websites, email, fax, verbally (over the phone) or mail delivery: a. Primary Source Websites – Verifications from primary source websites will show the name of the source, the provider(s) being verified, the type of verification (license, certificate, etc.), and expiration date if applicable. b. Email – Verifications received by email will be from an approved source and verify a provider's name, type of information being verified, and relevant start/end/expiration dates if applicable. c. Fax – Credentialing verifications received by faxes are automatically routed into a fax server. An assigned OMAG staff person will upload these to the appropriate provider's credentialing file as necessary. d. Verbal – Verifications from verbal sources are recorded electronically and will note the source, date of verification, type of verification, name of the individual verifying the information, their position and any relevant dates (certification, licensure, training, educations, etc.) e. USPS/FedEx/UPS – These verifications are delivered to OMAG. Verifications are then scanned and auto-dated when they are uploaded to the electronic file and stored securely electronically. Original hard copies may be securely destroyed once the verified scanned version has been uploaded into a file.
When and how documents get dated.	Documents uploaded to a provider's credentialing file are automatically dated electronically and the name of the staff member is included with on the PSV based on the individual who uploaded the item.
Who reviews the information.	One of our OMAG auditors must review the initial or reappointment applications along with all uploaded verifications to deem the file as *audit complete.* If necessary, a manager can also review in an auditor's stead as back-up.

How information is tracked.	File progress is tracked via TaskMaster credentialing platform and the ECHO electronic database. All verifications are uploaded into TaskMaster system to supplement the provider's credentialing application for initial or reappointment. The combination of these materials is referred to as the Provider Assessment Packet (PAP). After the PAP is reviewed by our file auditor, the PAPs are then reviewed again by our Credentialing Performance Improvement (CPI) team as they prepare the file for review by clinical leadership, prior to review by a Credentials Committee. When the provider's applications are finally approved by the requisite committee or governing body, the PAPs are then finalized as PDF packets which live in our ECHO credentialing system as historical records for review as necessary.
How/where information is stored.	The finally approved PAPs (including all verifications) are saved within the ECHO credentialing database upon final decision from the appropriate committee or governing body. Primary source verification storage procedures include the following: a. Verification responses are uploaded to our electronic file room and securely stored electronically (on mcmssowap001 server). b. Any printed verifications are locked in file drawers until a scan may be uploaded. Once scanned, verifications are then securely shredded. c. Provider's application processing is tracked through the UC Me file processing system. This is located on (on mcmssowap001) secure server and accessed through individual accounts assigned by our IT Programming Administrator based on unique user's UCSF LDAP NetID user accounts. d. The applications for visiting providers are scanned and stored in a secure server (\\fsmcb02\medical staff office\medical staff office\visiting applications). Original hard copies may be securely destroyed once the verified scanned version has been uploaded into a file.

CR 1.C.2. Tracking, dating, and modification of Information (CR1. Element C #2) How the organization tracks modifications made to credentialing information	
When the information was modified	It is not our policy for any credentialing staff to modify PSVs to a provider's initial or reappointment application. When a verification contains discrepant information or requires additional clarification, the credentialing staff clarify directly (with the provider or appropriate verifying source) via email, and include a copy of the PDF email string as uploaded supplemental documentation to the provider's PAP. Auto-generated system audit logs will randomly select active provider records for periodic analysis of modifications within the ECHO credentialing database. Credentialing team members involved in this audit process will review modifications and document the findings.
How the information was modified	Staff do not modify PSVs. They may only clarify verified information from the provider directly or appropriate verifying source.

	For verbal verifications, a memo to the file (or email from the processor) is included in the PAP as PDF supplemental documentation which will include the name and title of the individual completing the verification/clarification.
Staff who made the modification	All staff who clarify discrepant information upload a PDF copy of the communication with their name and date automatically uploaded to the provider's PAP.
Why the information was modified	Uploaded supplemental documentation from the credentialing staff will indicate the reason that the team member is requiring additional clarification.

CR 1.C.3. Authorized Staff for Reviewing, Modifying, And Deletion of Data (CR1. Element C #3) The policy must identify:	
Level of staff (title, job role) who are authorized to access, modify, and delete information.	ECHO credentialing database access for the Office of Medical Affairs and Governance Team is determined by department management and administered following each new employee's onboarding. Database access is predicated upon active UCSF LDAP authentication and account setup requests must be made in writing to the Manager for Departmental Applications, IT - Business /Clinical Systems. For the UCSF Office of Medical Affairs & Governance, the following applicable database security groups exist within the ECHO Credentialing Database. **A. ECHO Security –** System administrators only (full system access) **B. Administrator –**Access to system settings such as scheduling jobs **C. Manager – A**dditional feature to any group to review and audit ECHO system **D. Medical Staff (team) – Full read/write access to ECHO system (modify & delete)** **1. Audit Trail –** additional feature available for standard ECHO users **2. Privilege Form Maintenance** – additional feature, configure privilege forms **E. Read Only** – cannot modify system data All OMAG ECHO users are assigned (level D - medical staff) read/write ECHO credentialing database system access as necessary to perform their duties which includes modifying and deleting ECHO database credentialing information. Additional featured levels may be assigned to managers/supervisors based on an as needed basis to execute the essential functions of their role(s). Those levels include B – Administrator and C – Manager. Audit trail security level and privilege form maintenance levels are assigned to staff on an as needed basis to execute the essential functions of their role(s). Verifications received are uploaded to the electronic credentialing file and automatically dated in real time with the upload date and/or reviewed date along with the unique user's name who reviewed and uploaded the document.

	Each modification to a provider's ECHO credentialing profile are tracked by a system audit log which records the unique user, date of change, type of change, new data, and prior data in the field.
Circumstances when modification or deletion is appropriate. Organization must determine when it is appropriate and inappropriate to modify information in either electronic data and/or paper documents as applicable. Policies and procedures should include a comprehensive description of all appropriate modifications, if/when deleting information may be acceptable and what level of staff (role, title) have rights to modify what information.	Verification information may be modified by Credentialing Specialists, Supervisors or Managers when verification information changes – examples include but are not limited to (see below). As credentialing information changes, verifications are obtained to support such changes. Verifications uploaded into the Echo Credentialing Database include the uploader's identity, date, time, and location where the verifications are stored (either in the database itself or on our shared drive). There are rare, few circumstances when staff should be deleting primary source verification data in the ECHO credentialing database. Staff are trained to update ECHO credentialing database information as appropriate. Examples includes (but are not limited to) entry of new provider credentialing information to build credentialing profiles for new, incoming providers to be credentialed with UCSF Medical Center/UCSF Medical Group. Additionally, the team is required to update/modify ECHO credentialing data to ensure expiring licenses and other expirables monitoring data is up to date. Authorized users are recommended to check with their direct manager when a need to delete information presents itself. This includes instances when a PSV needs to be re-run to accurately reflect a provider's profile. **Examples of appropriate modifications to credentialing information** include but are not limited to: • Updates to expired licensure or other documents • Changes/updates to education, training, or privileges • To correct data entry errors • Addressing/identifying duplicate provider database profiles • Documents appended to incorrectly provider profiles **Examples of *inappropriate* modifications to credentialing information** include but are not limited to: • Altering credentialing approval dates that were not sanctioned by the Governance Advisory Council (GAC) or temporarily approved by the clinical leadership while awaiting GAC final approval • Altering dates on verifications cannot be performed • Whited out of dates or signatures on hard copy documents • Unauthorized/inappropriate deletion of provider files or supporting documentation

CR 1.C.4 Security Controls to Protect Information from Unauthorized Modification (CR1. Element C #4)
The policy must describe the process for:

Limiting physical access to credentialing information, protecting the accuracy of information gathered from primary and approved sources. Physical access may include, but is not limited to, servers, hardware, and physical records/files	Our physical servers that store our ECHO credentialing database and provider information is located at an offsite UCSF datacenter in an undisclosed location. Those with direct access include database administrators (DBA), the server team, Programmer/Database Developer, and the IT – Business/Clinical Systems team. All users can access the information stored on these servers only when located on site while directly on the UCSF network, or through VPN via our Pulse Secure (DUO), our multifactor user authentication security control. Only authorized individuals have access to the UCSF credentialing database and digital workspace (TaskMaster). Credentialing supervisors/managers work in conjunction with IT Security, IT Business/Clinical Systems, and the OMAG IT Programmer to enable appropriate access for appropriately identified staff. Only appropriately identified staff are allowed access the above referenced credentialing systems. Credentialing systems are hosted in the organization's secure intranet and are password protected to allow access to only authorized individuals. a. Initial user access is granted first through the UCSF Medical Center Account Request Form (ARF) system to ensure user's NetID is appropriately configured with the necessary access required. b. Subsequent ancillary system access is then determined with and requested from the IT Business/Clinical Systems and the OMAG IT Programmer to enable identified authorized user access based on the existing business need. Credentialing staff securely access all electronic credentialing practitioner files and information through the ECHO credentialing database or Taskmaster platforms. Hard copy data (such as any printed confidential/sensitive document or file) must be stored out of sight and not be accessible to anyone who does not have a business need to view the contents. Any provider files that are printed as hard copies should be housed in locked cabinets in a restricted area that is only accessible to authorized staff when not in process and during non-work hours. When hard copies of any credentialing documentation is no longer needed, the paper should be shredded or dumped into secure bins for shredding. Workstations are accessible only via unique user logon username & password. Workstation default settings entail a timeout after 15 minutes of inactivity to the login screen as additional security precaution. This feature cannot be changed or inactivated. Staff are encouraged to always log out to their PC's lock screen whenever stepping away from their workstation. Furthermore, computer screens should be positioned to prevent viewing by unauthorized individuals. Our credentialing systems are hosted in the organization's secure intranet and password protected to only allow authorized access. Upon resignation or any separation from the UCSF Office of Medical Affairs and Governance, managers submit a UCSF Medical Center Account Request Form to terminate a user's access with OMAG as part of the off-boarding process.

	Requests to modify provider ECHO records are reviewed by our trained staff, before modifications are made to provider's live records in TaskMaster/UC Me or the ECHO live production database. Modification to the credentialing record is limited only to authorized staff OMAG team members. Unauthorized users are not granted access, and ECHO users are trained to only edit their provider's active records. Release of credentialing information is only provided with accompanying signed release of information from the provider. Releases should be signed within 180 days of the date received. Only information requested is provided with a valid signed attestation release from the provider. Only copies of items that a provider has shared directly with OMAG may be re-released to the provider if requested. All password-based systems (Network access/logon, ECHO, Taskmaster, etc.) on UCSF workstations effectively mask/suppress, or obscure the passwords so that unauthorized persons are not able to observe them (e.g. ••••••). Authorized users are prohibited from allowing others to access computer systems or restricted areas with their account, password, badge, or unique ID logon information. All staff are required to complete the periodic UCSF Cybersecurity training which includes information regarding password management and password protection information. (Please see attached module Exhibit B.) Authorized users must adhere to the UCOP and UCSF specific policies and protocols which exists to establish strong use of password security and maintenance. Please refer to the attached Exhibit A to reference UCSF Password standards. Users must adhere to protocols that establish and maintain login credentials and identify/permit individual account security. A default password is established for accounts created by the IT Support Desk which the new user is forced to change upon their first login attempt. This initial default password is communicated to the new user when the network active directory account and equipment are issued or assigned. User passwords are subject to the UCSF password policy, which details these additional requirements on exhibit A. In addition to the password requirement standards detailed in exhibit A, users are reminded that unique user IDs and passwords/passphrases should not be written down, left in plain view, and that use of unique passwords (reset at least every 90 days) should not be reused or recycled passwords/passphrases that have been used previously. UCSF policy (Exhibit A) recommends passwords updated/changed at least every 90 days. If users believes password, passphrase, or other uniquely identifying information has been compromised, they should either navigate to https://password.ucsf.edu to have the password changed/updated. Users are also recommended to use different passwords/passphrases for different accounts, and should avoid writing down passwords/passphrases. If user has a problem changing their password, they submit a request to UCSF IT Support Help Desk at 415-514-4100 to have their password reset. Support Desk staff authenticates the user, by confirming the unique UCSF-provided

	Employee ID number assigned. Once the request has been verified, the administrator resets password to a default which is provided to the user and the account is set to force password change upon user's first login attempt. Terminations and transfers - User credentials are disabled when the staff member terminates employment from the UCSF Office of Medical Affairs and Governance, or transfers employment to a different department within UCSF. Authorization to access servers, databases, ancillary systems and files are removed upon transfer of staff from the OMAG department. Such a termination of access is conducted via UCSF Medical Center Account Requests Form (ARF) with the selection of either: • Modify existing account – for internal UCSF transfers; or • Terminate existing account – for individuals leaving UCSF altogether **Examples describing instances when credentialing information may be released:** Credentialing information would be shared through the following process/requirements to do so: • Requests from Risk Management, UCSF legal counsel (including retained outside counsel), Credentialing Committee Chair, Department Chairs or designees, etc. • Regulatory or accreditation agencies – specifically, records may be viewed via electronic desktop audit with direct supervision by an OMAG staff member to ensure no data is accessed without authorization. • Third parties or organizations (health plans, MCOs, etc.) with whom delegate is contracted. Each provider must have an appropriate signed authorization and release form on file. Records may be viewed via electronic desktop audit, following the completion of signing the OMAG confidentiality statement and with direct supervision by an OMAG staff member to ensure no data is accessed without authorization.

CR 1.C.5: Credentialing Process audit for factors 1-4 How the organization monitors its compliance with its own policies and procedures for credentialing system controls that address factors 1-4 at least annually and takes appropriate actions when applicable.
Our OMAG Credentials Verification Office (CVO) internally audits all OMAG initial and reappointment applications processed by our staff to ensure completeness and accuracy. When discrepancies are identified by our auditors, they are returned back to the assigned processor for further processing. When submitted files meet our OMAG file checklist processing standards, then our auditors may deem the file audit complete for next-step (review/routing) handling by additional members of the team. Our team has auditors that are specifically designated to review each file. Occasionally for coverage purposes or high volumes of files that require auditing, additional managers or supervisors may be assigned as auditors to review files for completeness and accuracy. Day-to-day auditor assignment is executed by the CVO Manager. Auto-generated system audit logs will randomly select active provider records for periodic analysis of modifications within the ECHO credentialing database. Credentialing team members involved in this audit

process will review modifications and document the findings. File audits are primarily conducted within the OMAG subgroup referred to as the CVO team. The CVO team is managed by the CVO manager, and reports to the Director for Credentialing and Privileging. UCSF Audit & Advisory Services is responsible for oversight to evaluate the effectiveness and efficiency for departments throughout UCSF, including the Office of Medical Affairs & Governance.

The OMAG CVO team's process is to deem a file as '*audit complete*' prior to releasing the file to the team responsible to ushering the file through the monthly committee review process. The existing process requires the initial or reappointed applications to be audit complete as a prerequisite to advance the file for further review and any subsequent recommended approval. 100% of files must follow this process and the (audit completion) status is recorded in our internal OMAG software called Taskmaster. Our CVO team auditors are typically responsible for reviewing and deeming the file as audit complete. However, as necessary for coverage purposes or high volumes of files that require auditing, additional managers or supervisors may be assigned as auditors to review files for completeness and accuracy. When assigned auditor for any application (initial or reappointment) is completing the file review audit, then each application is reviewed to ensure that the Taskmaster program has documented:

- the file reviewer;
- that the documents are all automatically dated by the TaskMaster program (upon upload)
- the applications and subsequent verifications are all appropriately documented within each record
- ensuring the Taskmaster system has a PAP created

Primary source documentation uploaded into our ECHO credentialing database cannot be modified. An annual review sampling 5% of active records or 50 files will be reviewed at random from our monthly health plan roster (provider universe) and conducted by department management/senior staff to ensure that the ECHO provider records are complete and possesses accurate information.

An annual review of active TaskMaster and ECHO user accounts may be pulled in order to ensure only authorized users continued to be listed on the requested report, no less frequently than annually. OMAG leadership will work with IT Clinical Business Systems staff to coordinate a periodic pull of this report of authorized, active ECHO user accounts. Additionally, OMAG Staff are required to complete their cybersecurity training annually.

CR 1.D Credentialing System Controls Oversight (CR1. Element D)	
Factor 1: Identify all modifications to credentialing and recredentialing information that did not meet the organizations policies/procedures for modifications as described in CR 1, Element C, Credentialing System Controls.	As a result of auditing our CR 1 C 1- 4 processes (no less frequently than annually), we will document whether there were modifications that did not meet our existing department's standards. This oversight will be completed at least annually, based upon automatically system generated reports that the team will be sent each month. Use of the Monitoring_Reporting_Innapropriate_Mod_Report.xls will be used to record instance of modifications that did not meet our existing department's standards

Factor 2: Document and analyze all modifications that did not meet standards by doing a qualitative and quantitative analysis of all modifications.	Qualitative analysis: The team will review those modifications that did not meet our existing department's standards to determine the root cause for the change. If deficiencies are identified, they may be escalated to the OMAG managers group to review and address based on level of concern/severity. If opportunities are identified for improvement of existing processes, then recommendations will be forwarded to the appropriate area manager(s). Quantitative analysis: When three or more inappropriate modifications of the same variety or theme have been identified, they will be they will be escalated to the OMAG managers group to review and address for a written plan to prevent further instances. The written response from the OMAG managers group should draw conclusions about the results and include follow-up action describing how to prevent further instances.
Factor 3: Acting on all findings. (Not applicable if no findings above.)	Any action determined from the previous (Factor 2) description will be documented within the Monitoring_Reporting_Innapropriate_Mod_Report.xls On the following scheduled basis (February 15, May 15, August 15, November 15) the team will review any actions determined from Factor 2 to assess for effectiveness. Continued monitoring will persist until improvement has been demonstrated for 3 consecutive quarters. If improvement isn't demonstrated for at least one finding, submit all quarterly reports.

Responsibility

Questions concerning this policy should be directed to the UCSF Office of Medical Affairs and Governance (OMAG) (415) 885-7268

History of Revisions

Revisions August 2022 UCSF Credentials Committee – updated language for elements CR1 C 1-4, addition of language for CR1 D, and addition of Addendum B – Credentialing Systems Control Oversight Tool

Revisions approved January 2022 UCSF Credentials Committee (reformation of elements 1 -4, rewriting of element 5, and addition of Cybersecurity training module exhibit)

Revisions approved June 2021 UCSF Credentials Committee (Details added throughout entire policy, including UCOP, UCSF, & Medical Center specific references)

Reapproved January 2021 by UCSF Credentials Committee (Section D, 1, e addition)
Initially approved November 2020 by UCSF Credentials Committee

Addendum A – Unified UCSF Enterprise Password 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

Addendum B – Credentials System Control Oversight Tool

Credentialing System Controls Oversight Report

NCQA (National Committee for Quality Assurance) requires the Health Plan to monitor our delegated entities to ensure appropriate oversight of their credentialing system security controls, as outlined in CR 1 Element C and D. Please complete the form below and return it, along with a monitoring report if any modifications were identified that did not meet your criteria outlined in your policies, procedures and/or delegation agreement.

Delegate Name: Click or tap here to enter text.
Delegate Person /Title who conducted Oversight: Click or tap here to enter text.
Date of Oversight: Click or tap here to enter text.
Time period of oversight: Click or tap here to enter text.
Delegate uses: ☐ **Electronic System** ☐ **Paper Files** ☐ **Both**

Auditing Frequency: (Check one box) ☐ Monthly ☐ Quarterly ☐ Semi-Annually ☐ Annually ☐ Other(explain) Click or tap here to enter text.

CR 1 Element C - Credentialing System Controls Oversight

Please complete the below fields to show your oversight of Credentialing System Controls Factors 1-4: REQUIRED

Standard	Provide a brief description of the method utilized to ensure compliance with your policies/procedures for the following elements.	**Results of review** No findings/findings (explain)	**Follow up on findings** (if applicable)	**Comments**
CR 1- C1 Primary Source Verification				
CR 1- C2 Tracking Modifications				

CR 1- C3 Authorization to modify information				
CR 1- C4 Securing Information				

CR 1 Element D - Credentialing System Controls Oversight
TYPE(s) OF SYSTEM

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

☐	Our Credentialing System does not allow for modifications under any circumstances. Please note, if selected: Your policy and documentation need to be provided that describes the functionality of your system to ensure modifications are not allowed.
☐	Our Credentialing System allows modifications only under specific circumstances established in our policy and we monitor compliance with the policy.
☐	Our system uses system alerts/flags to identify noncompliance.
☐	Our system is not able to identify any modifications and/or we use paper files (All credentialing files (or a sampling of 5% or 50 files) are audited for non-compliant modifications)

CR 1 Element D - Credentialing System Controls Oversight

Select if *NONCOMPLIANT* modifications were identified during the review period. A report of all the identified noncompliant modifications needs to be submitted. (template report is attached)

☐ 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.

CR 1 Element D – Credentialing System Controls Oversight

Select if all modifications reviewed were *COMPLIANT* during the review period. Otherwise, you are required to submit a report of all noncompliant modifications.

☐ 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.

_____

Signature of Person Completing the Report

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

_____

Date