KERN HEALTH SYSTEMS POLICY AND PROCEDURES			
Policy Title	UM Referrals System Controls	**Policy #**	30.52-P
Policy Owner	Utilization Management	**Original Effective Date**	7/2024
Revision Effective Date		**Approval Date**	01/28/2025
Line of Business	☒ Medi-Cal ☐ Medicare		

I. PURPOSE

To define Kern Health Systems (KHS) policy and procedure that adheres to system controls for utilization management referral processing, as required by State and Federal regulatory requirements and NCQA standards.

II. POLICY

A. It is the policy of KHS that Utilization Management (UM) system controls and procedures are in place to protect data from being altered outside of defined KHS policies and procedures for UM denials notifications.

B. KHS shall adhere to Federal, State, and National Committee for Quality Assurance (NCQA) requirements to secure access to systems, define role-based permissions, and ensure that UM and System users work is tracked and auditable.

   1. Monitoring of these standards occur through Information Technology (IT) Security Risk assessments and internal UM data validation audits and monitoring reports conducted by designated Utilization Management (UM) staff not involved in UM referral or processing.

C. KHS shall maintain established requirements for the configuration management and ongoing management of Utilization Management (UM) referral systems by maintaining adequate controls and monitoring processes to safeguard the UM processes as follows:

   1. No decision-making and practices on the use of the referral system, including upgrade requests, can be configured without, but not limited to, Quality Improvement (QI), UM and Compliance sign-off.

   2. Role Based Access Control: KHS UM staff are assigned specific sign-on roles based on user department functions and credentials.

   3. All UM staff will undergo training on the use of the system application and process.

D. UM Staff Levels for Decision Making

1. UM Staff apply evidence-based criteria to requested services and approve when criteria have been met. In the event criterion is not met, UM Staff prepare case review to the UM medical physician reviewer or behavioral health reviewer, (Doctor of Medicine (MD) or Doctor of Psychology (PsyD)) for determination of medical necessity. All cases reviewed by the MD or PsyD will be evidenced by an electronic date stamped signature.

2. UM Nurses utilize medical necessity criteria and clinical practices guidelines in the determination of inpatient/outpatient member care management. UM Nurses are active Registered Nurses or Licensed Vocational Nurses who may approve an inpatient or outpatient referral based on clinical information, medical necessity, and appropriate medical criteria. Case Managers do not make decisions for denials or modifications.

3. UM Coordinators are non-clinical employees with medical terminology training, medical office experience, or other related experience. UM Coordinators screen in-coming authorization requests, create referrals received via fax, phone, or mail, verify eligibility and benefits, and prepare necessary information and medical records for clinical review. UM Coordinators approve specific benefit authorizations at the approval of the Chief Medical Officer (CMO); they are not involved in any decision making that requires clinical judgment. Licensed staff employees supervise all review decisions.

4. Upon completion, all UM referrals are stamped with the date, time and name of the authorized personnel who made the final entry determination status of approved, modified, or denied.

III. DEFINITIONS

TERMS	DEFINITIONS
Action date and time	Date of Receipt: The date when the referral arrives at KHS, even if it is not received by the UM department.
Re-Opening	A remedial action taken to change a final determination or decision even though the determination or decision was correct based on the evidence of record.
Date of Written Notification	Date of written notification is considered as the date on the written notice.
Date or Verbal Notification (if applicable)	Verbal notification is considered delivered on the date/time KHS representative speaks directly to or leaves a voicemail for the member or their authorized representative (e.g., legal guardian, or other formally named representative).

IV. PROCEDURES

A. KHS has designated date and time fields within the referral system that are auto locked upon data entry. These fields are as follows:

   1. Member and Provider Approval Notification date and times
   2. Referral received date and time.

B. The KHS UM information system tracks all edits or alterations to the electronic UM referral record. Only those afforded permission by role may edit an existing record under specific circumstances. Information Technology staff assure appropriate security access to the system via policy and procedures.

C. In the event an error is made in entering a received date for an authorization request that is manually entered and does not match the automated UM system date and time stamp assignment and/or UM determination, it will be corrected within the UM System as a note by designated permissible staff to include the reason for the change.

   1. Any instance of a manual error upon entry by the UM staff during a creation of a case into the UM system, the case is voided/canceled, and the UM staff creates a new entry, documenting both referral numbers in each case to allow transparency for each request.

   2. KHS has a self-reporting process that allows UM staff to alert UM management and compliance of the initial error. The process will be tracked in the system and will be reflected in the UM daily monitoring report.

   3. If the error is system generated, the UM leadership will intervene and work with the UM Department to ensure the correct received or notification date is documented.

D. System controls and Configuration are a two-tier process.

   1. Tier I: Information Technology (IT) configuration
      a. IT maintains the development, documentation, and maintenance of the referral system at an enterprise-level (e.g., operating systems, databases, middleware, enterprise applications, etc.) within its environment.
      b. Reviews and updates at least annually or as needed any system upgrades, patches, or other significant changes.
      c. Retains a record of previous configurations through Change Requests Logs.
      d. Establishes the UM referral system configuration or components with elevated security controls when a device is used to access the referral system.
      e. Develop, document, and maintain agency-specific referral system configuration.
      f. Configuration Change Control
         i. Determine the types of changes to the UM referral system that are configuration controlled.
         ii. Review proposed configuration changes and approve or disapprove with explicit consideration for security impact analysis and document change decisions.
         iii. Test, validate, and document planned changes prior to implementation of

approved changes.

iv. Retain records of changes for the life of the system and retain audit and review activities associated with changes. All change requests establish timelines and changes. Formal procedures are being developed for institutionalized documentation.

v. Coordinate and provide oversight for change control activities.

g. Security and Access

i. Security and access are configured within the system based on the user role within the application.

2. Tier II: Utilization Management (UM) Security and Access
   a. Establish, define, and document configuration settings for user roles and functions.
   b. Identify, document, and approve any access request for the UM referral system UM modules.
   c. Monitor and control changes implemented by IT in accordance with desktop level and department policies and procedures.
   d. Only the UM Director or designated UM leadership are authorized to modify dates under specific circumstances and will document in JIVA as part of the UM denials trail.
   e. Circumstances when modification is appropriate.
      i. Changing receipt data due to entry error
      ii. Changing notification date due to data entry error

E. Referral date and time starts at the time of receipt by KHS.

1. Provider portal: Date and time referral is submitted into the referral system automatically.
2. Fax, Mail, and Telephone: Date and time the referral is received via the successful fax transmittal receipt, mail date and time stamp are manually entered.
3. Case entry date and time is when the case is created in the UM module Jiva by the UM staff. Notification date and time recording is as follows:
   a. Member Notification: The written notification date is the same as the decision date.
   b. Provider Notification The written notification date is the same as the decision date. KHS uses the date on the notice as the notification date.
   c. KHS uses the date when the notification was posted in the electronic system.
   d. A portal notification date and time is automatically populated into the corresponding data fields derived from the decision date.

F. System tracking

1. Dates - All main records are date-stamped based on the creation date along with the change date.
2. Audit trails - System stores audit trails to track the changes in status and key fields within each module. Tracking includes:
   a. Date of modification.
   b. Who modified the date.
   c. Reason date was modified.

G. Securing System Data

1. KHS audits the processes as mentioned above and/or procedures as follows:
    a. Business Intelligence (BI) department, in collaboration with the UM Director, utilizes both an automated mechanism and a manual process. This is conducted on a quarterly basis to assess effectiveness of actions on all finding until demonstrated improvement for one finding over at least consecutive quarters.
    b. Automated process includes reviewing predefined data points.

2. Tools and Services:
    a. Monitor SQL Servers
        i. Spotlight and Database Performance Analyzer (DPA) are used to monitor Applications and services.
        ii. Manual process includes having various IT designees tasked with specific functions to monitor the status of jobs at designated timeframes.
    b. The IT system checks are towards:
        i. System – System Center Operations Manager (SCOM), and Paessler Router Traffic Grapher (PRTG), and Manual Process.
        ii. Application – SCOM and PRTG and Manual Process
        iii. Data – Spotight and DPA and Manual Process
        iv. Reporting – SQL Sentry and Manual Process

H. UM Denial Systems Control, Compliance Monitoring and Oversight:

1. KHS has a process of reviewing automatic system alerts or flags for date modifications or events in real time, a quarterly process for assessing effectiveness of actions, and a separate process for annually testing performance of the system's automatic alerts or flags. Appropriate actions will be taken accordingly.

2. KHS monitors compliance with its UM denial controls by:

    a. Identifying all modifications to receipt and decision notification dates that did not meet KHS policies and procedures for date modifications.
    b. Analyzing all instances of date modifications that did not meet the date modifications policies and procedures.
    c. Acting on all findings and implementing quarterly monitoring process until an improvement is demonstrated over three consecutive quarters.

3. The UM Director is responsible for the oversight and reporting of the following monitoring processes:

    a. Modifications that did not meet policy and procedure.
    b. Analysis of modifications being made.
    c. Actions taken on modification that did not meet policy and procedure.
    d. Quarterly review & follow-up to track improvement, if applicable.

4. Daily Monitoring Process:

   Every UM staff member adheres to a self-reporting process that allows the employee to report to Compliance and UM Management when a breach in the policy is identified.

   The UM Department has a daily monitoring report in place to capture inappropriate or unauthorized modifications. The UM Director and designated UM leadership will review the system-generated report from the UM system, JIVA; a comprehensive listing of all date modifications to identify modifications that did not meet the policy and procedure. All non-compliant modifications are reviewed, which include correcting typographical errors, deleting information, changing receipt and notification dates, or creating a new record in place of an existing record.

   The UM Director and designated UM leadership will aggregate the results of the daily monitoring report, which will include the number and percentage of non-compliant files.

When Unauthorized Modifications are Identified

a. When the UM Director is notified of an unauthorized modification, either by self-reporting or by the daily monitoring report, the UM Director or designee works with the staff, direct report, and the individual to review the process and policy to assure an understanding and provide any education identified. Any UM staff with three (3) or more unauthorized modifications are monitored more closely to assure compliance with the policy.
b. The UM Director or designee will conduct training with all UM staff who have permission to manually enter dates received via mail, fax, verbally by phone, or verbally via voice mail regarding correct and accurate manual entry of dates, verification of member or creating case numbers on initial entry into the system.
c. The UM Director or designee will educate the UM staff at least annually regarding the requirements of this policy.

5. Quarterly Monitoring:

   To determine the effectiveness of the corrective action:
   a. The UM Director will review the aggregate daily monitoring results from the previous three months from a system-generated report of all date modifications to identify patterns of non-compliance for three consecutive months.
   b. The UM Director will perform quarterly monitoring until it demonstrates improvement for one finding over three consecutive quarters.
   c. The UM Director will submit the report quarterly to the Quality Improvement Health Equity Committee for recommendations or follow-up actions. The report will be presented with the Quarterly HICE Report and will track the following:
      i. Raw # of dates modified – review of the # of cases with date modifications.
      ii. # of dates with non-compliant modifications
      iii. % of dates of non-compliant

6. Annual Monitoring

    a. Annually, the UM Director will conduct quantitative and qualitative analysis report on UM denial modifications, and this will be a part of the annual UM evaluation.
    b. Additional safeguards are provided by conducting an annual testing of the performance of the system's automatic alert system or flags to review date modifications or events in real time. Action will be taken to update the referral UM system controls accordingly.

I. Security Controls to Protect Data from Unauthorized Modification:

1. Limiting Physical Access

    a. Only staff authorized by the CIO and Director of Information Technology are granted access, via physical ID badge, to secure locations that house KHS computer servers, hardware and physical records and files. Physical access to provider files stored in the electronic UM drive and UM software are accessible to only authorized individuals who require access based on business need.

2. Preventing Unauthorized Access:

    a. KHS installs and maintains a firewall configuration to protect sensitive information as detailed in KHS Policy and Procedure 70.49-I: Firewall Policy. Only authorized individuals have access to KHS UM system database and UM folder. Access is determined and granted upon hire for job necessity for having access to the UM system. The UM Director works in conjunction with IT Security to enable appropriate access for appropriately identified staff. The UM system is hosted on the KHS secure intranet and password protected to allow access to only authorized individuals. Electronic UM files are maintained on a secure server that requires individual authorization to access the information. Electronic communications receive the same protection as previous hard-copy documents regarding confidentiality and disclosure policy.

    b. KHS' IT Department has a 2--Tier process for system controls and configuration, as described in Section D, page 4 of this policy.

3. Password-Protecting Electronic Systems:

    a. All password-based systems on KHS workstations are designed to obscure the passwords so that unauthorized persons are not able to observe them. Authorized users are assigned unique username and are given the ability to create unique and strong password utilizing upper- and lower-case characters and special characters. Grace login after a required password change is allowed once, thereafter the system is locked, and staff must contact the UM Director to reset password. Staff are instructed to avoid writing down passwords and passwords must be changed immediately if the user suspects their unique password to be compromised. Role-based security prevents unauthorized access to information and unauthorized modifications to information within the credentialing software through the grouping of users based on job description. The UM Director is responsible for the maintenance of UM system users and groups.

4. Passwords/User IDs IT Password requirements

The following minimum parameters must be met to ensure a strong password:

a. At least twelve (12) characters.

b. Not based on anything somebody else could easily guess or obtain using personal related information (e.g., names, telephone numbers, dates of birth, etc.).

c. Not vulnerable to a dictionary attack (see Recommendations for Creating Compliant Passwords section).

d. A combination of at least one character from each of the following fourlisted character types:

i. English uppercase letters (A-Z),

ii. English lowercase letters (a-z)

iii. Base 10 digits (0-9)

iv. Non-alphanumeric (such as but not limited to ` ~! @ # $ % ^ & * ( ) _ + - = { } | \ : " ; ' < > ? , . / And space)

e. Passwords must be changed regularly.

i. According to recommendations made by NIST and Microsoft, passwords are not frequently changed unless anomalous activity is discovered. IN addition, KHS utilizes a DLL that validates prior use or compromised passwords further supported with Multi Factor Authentication.

ii. Passwords must not be reused for at least twenty four (24) generations.

iii. Passwords are reset when requested by staff or if passwords are compromised.

f. User IDs and password are unique to each user.

g. Individual User Responsibilities

i. Passwords must never be written down and left in a location easily accessible or visible to others. This includes both paper and digital formats.

ii. Different passwords should be used for different accounts.

h. Disabling or Removing Passwords

i. When an employee leaves the organization, the Human Resources department will notify the IT department of the date and time of the employees exit from the organization. At that time, IT will disable the users account, including all passwords.

J. Recording Dates

Entering the received date for faxed, provider portal, verbal request, or mailed requests. The date of receipt is the date/time used to note the date/time a request was made for UM service request.

1. If received by U.S. mail, the date/time the document is physically received at the KHS place of business.
2. Internal UM mail is manually date time stamped by the KHS designated mail room staff and this mail stamp is manually entered by the UM coordinator.

   a. Internal UM mail is manually date time stamped by the KHS designated mail room staff and this mail stamp is manually entered by the UM coordinator.
   b. If received by fax, the date/time indicated by the fax transmission report.
      i. This is recorded through Scanfinity and manually entered by the UM coordinator.
   c. If received verbally by phone, the date/time the call was made with the request.
      i. The coordinator in real time during the call verifies eligibility and creates a case number entering the date and time.
   d. If received verbally by voicemail,
      i. The date/time the initial message was left in the voicemail system is manually entered by the UM coordinator.
   e. If received through the provider portal the date/time stamp recorded in the portal as submitted and systematically entered in the system.
   f. The veracity of the date and time entries are audited by comparing:
      i. The scanned images of the requests Fax-Portal as applicable to the time entered in Jiva.
      ii. Reviewing the mail stamped date and time to the entry.
      iii. Pulling the phone call data-date and time.
   g. Envelopes are retained with the UM referral correspondence.

K. Protection Controls

1. Each entry associated within a referral is stamped with the date, time and name of the authorized personnel who made the entry.

2. No UM personnel can change a date and time once it is entered except when certain circumstances require appropriate modification as listed in page 4, Section D # 2. Only the UM Director are authorized to modify dates under any circumstances.

3. Updates are only made as a final determination of the medical necessity to update the case in final 'Auth Status" approved, modified, denied.

4. In the event any changes are required to an already adjudicated authorization, it is handled directly by the UM Director:

   a. The rationale for the change and the change itself will be documented by UM Director. This information is viewable within the audit trail of the referral.
   b. All changes will be trackable and monitored.

5. IT/Business Analyst will submit UM denial modifications reports to the UM Director on a daily basis.

V. ATTACHMENTS

Attachment A:	N/A

VI. REFERENCES

Reference Type	Specific Reference
Other	NCQA UM 12 – UM System Control
Other KHS Policies	IT Policies: 7.11-P Privacy and Security Policy; 7.27-I Employee User Access
Other KHS Policies	IT Policies: 70.49-1: Firewall Policy
Password Change Best Practices	https://learn.microsoft.com/en-us/microsoft-365/admin/misc/password-policy-recommendations?view=o365-worldwide https://community.trustcloud.ai/article/nist-password-guidelines-2024-15-rules-to-follow/

VII. REVISION HISTORY

Action	Date	Brief Description of Updates	Author
Created	7/2024	The policy was created to align with State & Federal regulations, and NCQA Standards.	C.P. Utilization Management

VIII. APPROVALS

Committees | Board (if applicable)	Date Reviewed	Date Approved
Choose an item.		
Choose an item.		

Regulatory Agencies (if applicable)	Date Reviewed	Date Approved
Choose an item.		

Chief Executive Leadership Approval *		
Title	**Signature**	**Date Approved**
Chief Executive Officer		
Chief Medical Officer		
Choose an item.		
*Signatures are kept on file for reference but will not be on the published copy		

KERN HEALTH SYSTEMS

Policy and Procedure Review

KHS Policy & Procedure: 30.52-P UM Referrals System Controls

Reason for Creation: The policy was created to align with State & Federal regulations, and NCQA Standards.

Director Approval		
Title	**Signature**	**Date Approved**
Christine Pence Senior Director of Health Services		
Dr. Maninder Khalsa Medical Director of Utilization Management		
Amanda Gonzalez Director of Utilization Management		

Date posted to public drive: _______________

Date posted to website ("P" policies only): _______________