

Guide to KPHC Access Provisioning of NCAL Affiliate Users

Kaiser Foundation Health Plan, Inc.

Ethics and Compliance

Privacy, Security and Technology Compliance

Version 1.0

December 3, 2021

Table of Contents

- 1. Overview4
- 2. KPHC Access Provisioning Process Flow5
- 3. KPHC Access Provisioning Procedures6
 - 3.1 Access Templates6
 - 3.2 Access Request Form7
 - 3.3 Contracts and Agreements7
 - 3.3.1 Licenses and Contracts7
 - 3.3.2 Business Associate Agreements7
 - 3.3.3 Confidentiality Agreements8
 - 3.4 Monitoring System Use8
 - 3.5 Affiliate User Training8
 - 3.6 KP Online Affiliate Registration9
 - 3.7 KPIM-AP9
 - 3.7.1 Approve Access 10
 - 3.7.2 Reject Request 10
 - 3.7.3 Offline Verification 10
 - 3.7.4 Suspend Access 11
 - 3.7.5 Revoke Access 11
 - 3.8 KPIM 11
 - 3.9 KP HealthConnect Security 12
- 4. Post-Provisioning Guidance 13
 - 4.1 How to Access Health Records 13
 - 4.1.1 KP Online Affiliate 13

4.1.2 Epic Hyperspace 13

4.2 Access and Monitoring Reviews 13

4.2.1 CARMA Access Review 13

4.2.2 NCAL iACT Monitoring Review..... 14

Appendix A: NCAL Affiliate User Onboarding Checklist 15

Appendix B: NCAL Area Compliance Officers 20

Appendix C: Contacts 21

Appendix D: References 22

Document Revision History 24

1. Overview

Kaiser Permanente (KP) allows certain authorized non-KP users a secure view into Kaiser Permanente HealthConnect (KPHC), KP's integrated care delivery and electronic health record system, which links members securely to their health care teams, personal health information, and the latest medical care provided by KP.

Access to KPHC may be granted, in accordance with the Access to Kaiser Permanente Electronic Information Systems for Non-KP Personnel Policy ([NCAL-PRIV-028](#))¹, to NCAL Affiliates who provide health care services to members and patients on behalf of KP.

This guide addresses the steps necessary to effectively provision, monitor, and deprovision KPHC access to NCAL Affiliate practitioners and other authorized personnel, as outlined below:

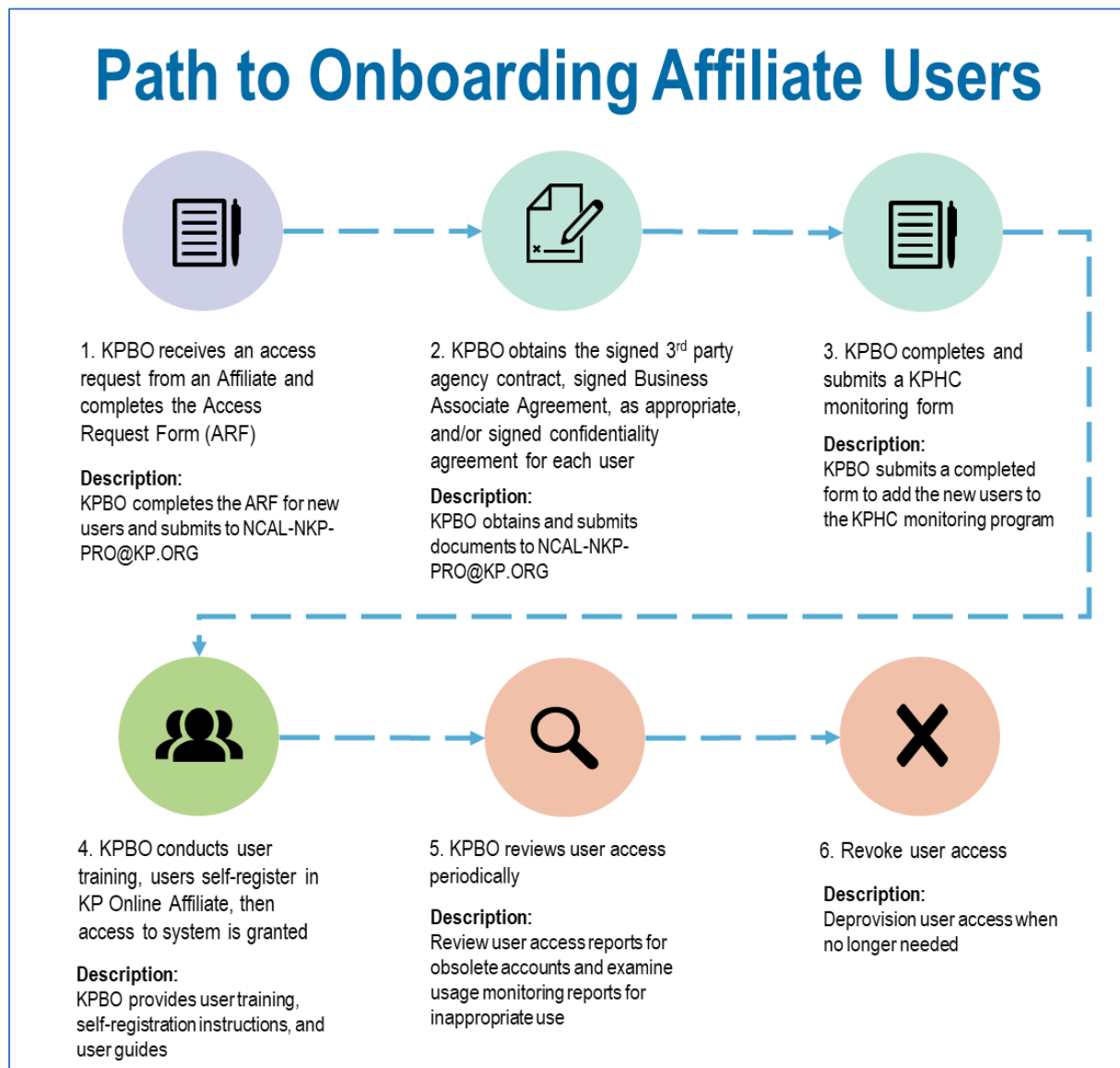
- Receive an Affiliate request for user access via the KP Business Owner
- Gather contracts, Business Associate Agreements, when applicable, and/or confidentiality agreements, as required
- Complete and submit information to monitor KPHC usage of new users
- Train, register, and grant access to new users
- Review user access and usage monitoring reports periodically
- Deprovision user access when no longer needed

The KP Business Owner (KPBO) acts as the liaison between the Affiliate management, Affiliate users, and KP System Administrators. The KPBO is responsible for the orderly and expeditious flow of the KPHC access provisioning process.

¹ The Access to Kaiser Permanente Electronic Information Systems for Non-KP Personnel Policy ([NCAL-PRIV-028](#)) will be converted to a Standard Operating Procedure (SOP) in 2022.

2. KPHC Access Provisioning Process Flow

The diagram below shows a visual overview of the KPHC access provisioning process:



3. KPHC Access Provisioning Procedures

Access Provisioning is initiated when an Affiliate group contacts the KP Business Owner (KPBO) to request access to KPHC which is necessary in providing health care services to members and patients.

The request typically includes the following information:

- Type of access required
- Business or clinical justification for the request
- Names of users who require the access

3.1 Access Templates

The type of access required determines the access template that will be applied to the request. This ensures the right level of access is granted to the user with visibility only to the KPHC records that will satisfy the business or clinical reasons provided. All templates include access to benefits, claims, and eligibility records. The template types are:

- Online Affiliate Template
 - [Affiliate Eligibility](#) – allows users access to benefits, claims, and eligibility records. It is the most common template applied program-wide. It does not include any clinical information.
 - [Affiliate Provider Read Only](#) – It is the most used template and includes access to clinical information.
- Epic Hyperspace Template
 - [Non-KP Provider Read Only](#) – allows users to access the clinical information of patients in KPHC.
 - [Non-KP Provider Read/Write](#) – reserved for users on KP sites (i.e., onsite transplants) that need to document directly into the KPHC. This is the least used template due to the expanded level of access.
- Special Request Templates
 - [Affiliate Provider Read Only MHCD](#) – reserved for users who provide mental health/chemical dependency (substance abuse) care to members and patients.
 - [Affiliate HH HO](#) – designed to accommodate Home Health providers. The home health/hospice template allows an expanded clinical view into KPHC through the

number of options and services available to NCAL KPHC users. It may also be appropriate for other groups as needed.

- [Affiliate SNF](#) – allows one of the highest levels of access and must **ONLY** be assigned to Skilled Nursing Facility users.
- [Affiliate Provider Surgery Center Staff](#) – reserved for Affiliate users who provide support on patient surgeries at designated Affiliate sites, in collaboration with KP physicians and other staff.

3.2 Access Request Form

Upon receipt of a request for KPHC access from an Affiliate group, the KPBO performs the following:

- Complete an [Access Request Form \(ARF\)](#) for the new Affiliate group.
- Submit the completed form to NCAL-NKP-PRO@KP.ORG with copy to the respective NCAL Area Compliance Officer. Refer to *Appendix B: NCAL Area Compliance Officers* for the list of ACOs.

3.3 Contracts and Agreements

The KPBO must obtain all pertinent contracts and agreements from the Affiliate group and submit the signed documents to NCAL-NKP-PRO@KP.ORG upon receipt.

3.3.1 Licenses and Contracts

The applicable signed agreements or contracts must be obtained from the Affiliate group:

- Obtain a signed [KP Contractor Affiliate Web Sites License – Provider Entity Agreement](#) – this required document must be signed by an authorized signatory who has the legal authority to bind the provider entity (and the provider employees).
- For Epic Hyperspace access, obtain a signed [KPHC Electronic Medical Record Access Agreement](#).
- For Mental Health/Chemical Dependency health information access, obtain a signed [KP Contractor Affiliate Web Sites License MHSA](#).

3.3.2 Business Associate Agreements

The KPBO must assess the need for a Business Associate Agreement (BAA). Most groups generally do not require a BAA.

To determine if a BAA is required, refer to [Business Associate Justification Log – Decision Tool](#). If required, a signed [Business Associate Agreement](#) must be obtained from the Affiliate.

3.3.3 Confidentiality Agreements

The confidentiality agreement outlines the requirements and expectations of Affiliate users that access the KPHC system. By signing the document, the Affiliate user agrees to the provisions of the agreement.

A signed [Non-KP Provider Confidentiality Agreement](#) must be obtained from each Affiliate user before access can be granted. This form applies to most users.

For users who need access to Mental Health and Chemical Dependency records, a signed [Non- KP Provider Confidentiality Agreement MHCD](#) must be obtained from each Affiliate user.

NOTE: Ensure users use consistent Group/Provider Name in the Location – Name of Hospital/Facility field when filling out the agreement.

3.4 Monitoring System Use

Kaiser Permanente has a responsibility to our members to preserve the confidentiality of their protected health information (PHI). An important aspect of granting Affiliate users access to our electronic information systems is to ensure that the access is limited by the principles of "minimum necessary" and "need to know" in accordance with the Uses and Disclosures of PHI and Minimum Necessary Policy ([NATL.EC.PRIV.014](#)). A means of ensuring compliance with this policy is to regularly monitor the use of KP systems.

Therefore, the KPBO must notify the NCAL iACT group, which monitors KPHC user access, when a new Affiliate user is provisioned in KPHC, by following these steps:

- Complete the [Non-KP Access Monitoring Report Form](#) and provide the NUID of the new user. Use the [Non-KP Access Monitoring Report Form for SNF/HH/HO Users](#) when provisioning Skilled Nursing Facility, Home Health, and Hospice users.

If the NUID is not yet available, resubmit the form when the user receives their assigned NUID. The initial submission provides NCAL iACT advance notice to initiate the monitoring workflow.

- Email the completed form to NCAL-RCO-iACT-Reporting@kp.org with a copy to NCAL-NKP-PRO@kp.org.

3.5 Affiliate User Training

The KPBO conducts the [Non-KP Affiliate User Training](#), which serves to familiarize Affiliate users with KP security and privacy policies and procedures including requirements for the safeguarding of protected health information (PHI). The training covers topics such as:

- NUID assignment
- Password requirements
- Storage of sensitive information
- Disposal of sensitive information
- Minimum Necessary Standard
- Communication with authorized care givers
- Security and privacy incident response guidance
- Workstation and remote access
- Access monitoring and auditing

3.6 KP Online Affiliate Registration

KP Online Affiliate provides Affiliate users a secure “read” access to electronic medical records of KP members for whom they provide care. The system is linked with KPHC, which connects our members securely to their health care teams, personal health Information, and the latest medical knowledge.

When all preceding steps in the access provisioning process have been completed, the KPBO provides the Affiliate group with the [KP Online Affiliate User Registration Guide](#). The guide shows an Affiliate user how to self-register their access request via the [NCAL Community Provider Portal \(CPP\)](#) and clicking on **Online Affiliate** then **Registration**.

Each new Affiliate user must register to obtain access to KP Online Affiliate.

The [KP Online Affiliate Bulk User Registration Guide](#) on the other hand shows authorized Affiliate group managers and administrative staff with Administrator-Level Access how to register several Affiliate users at a time by using a downloadable spreadsheet.

Affiliate users may at times require assistance from the KPBO when issues arise. Refer to the [Tips for the KP Business Owner \(KPBO\)](#) for guidance on common issues and how to troubleshoot them.

3.7 KPIM-AP

KPIM-AP² (<https://kpim.kp.org/kpim-ap/secure>)—a module of KP Identity Manager (KPIM) system—facilitates the provisioning of new user access at KP. It is the authoritative system that issues a unique National User ID (NUID) to each user who is authorized to access the KP network. An NUID is required to sign on to KP applications.

Authorized staff who support Affiliate users are granted access to the KPIM-AP queue which allows them to perform the duties of a System Administrator (SA). The SA manages the KPIM-AP queue and reviews the queue for provisionally registered KP Online Affiliate users who have requested access.

² Starting in Q1 2022, user access provisioning will occur in AccessNow, the new consolidated platform for identity governance service.

A new System Administrator may request access to KPIM-AP by submitting a [Directed Service Request](#) in ServiceNow, type in “**Access**”, click on “**Select a support group**”, enter “**ASG DRTAS KPIM SUP**”, and provide a detailed description of the request.

A new System Administrator will also need to request KPIM Support to add their email address to the distribution list to ensure the new System Administrator is copied on the Affiliate user approval notification email. To initiate this, submit a [Directed Service Request](#) in ServiceNow, type in “**Access**”, click on “**Select a support group**”, enter “**ASG DRTAS KPIM SUP**”, and provide a detailed description of the request.

Refer to the [KPIM-AP Administrator Guide](#) for guidance on managing the KPIM-AP queue.

3.7.1 Approve Access

When the SA identifies the Affiliate user in the KPIM-AP queue, the SA selects the ‘**Edit**’ option, reviews the request, assigns the appropriate Home Deployment (Capital, South Bay, North Bay, Golden Gate, East Bay or Central California), and ensures that the correct access template (as described in section 3.1 *Access Templates* of this document) is utilized in accordance with the provisions of the Affiliate licenses, contracts, and agreements. When this task is complete, the SA selects “**Done**”. Subsequently, the SA receives an acknowledgment from KPIM with the user’s NUID. The SA then informs the KPBO of the access approval who in turn provides the user their NUID. The user, at this point, can finalize the KP Online Affiliate registration as described in Page 10 of the [KP Online Affiliate User Registration Guide](#).

3.7.2 Reject Request

To decline a request, the SA identifies the Affiliate user in the KPIM-AP queue and selects the ‘**Reject**’ option. A pop-up comment box is displayed to allow the SA to add a comment, reason, or further instructions. Upon entering the information, the SA selects “**Reject**”, then notifies the user that the request has been rejected including the reason indicated. The user, with the help of the KPBO, will need to address the issue.

Besides other legitimate reasons, rejects can also occur when an unauthorized user obtains a copy of the registration packet and subsequently registers in KP Online Affiliate.

3.7.3 Offline Verification

When an Affiliate user attempts to register but is unable to complete the identity verification process, it may be due to the following reasons:

- The user answered the questions incorrectly.
- The user did not respond to the questions in the allotted time.
- The user has been referred for KPIM-AP Offline Verification.

When this occurs, the SA will need to access the KPIM-AP queue and select Offline Verification. The SA will also need to verify with the KPBO that the username and email address are accurate. Upon confirmation, the SA changes the level of assurance to 'Yes', which subsequently returns the request to the KPIM-AP Approval queue. The Affiliate user access provisioning can then proceed with the steps described in sections 3.7.1 *Approve Access* or 3.7.2 *Reject Request* above.

3.7.4 Suspend Access

Upon request from the KPBO, the SA can suspend a user's access by selecting the "Suspend" option, which inactivates the account thus preventing the user from signing on to KP Online Affiliate. The "Suspend" option is a toggle button and becomes a "Restore" option when "Suspend" is activated.

The KPBO should notify the Affiliate user when the access is to be suspended.

3.7.5 Revoke Access

Upon request from the KPBO, the SA can also revoke a user's access to their KP Online Affiliate account by selecting the "Revoke" option. When access is revoked, the user will receive a message at login that they are no longer authorized to access the system.

The KPBO should notify the Affiliate user when the access is to be revoked.

To restore access to KP Online Affiliate, the user must re-register by accessing [NCAL Manage Account](#) page and following these steps:

- Click on Provider Associations and Access and fill in the required fields.
- Select the access type "Clinical (includes administrative)" and click "Submit".
- Upon completion, the access request will appear in the KPIM-AP queue for SA approval.

3.8 KPIM

The KP Identity Manager (KPIM)³ (<https://kpim.kp.org/KPIM>) is a self-service application that provides authorized personnel the ability to request new NUIDs; review, approve or reject identity requests; request access to applications; extend or terminate contingent workers; and review contingent work status.

The SA or KPBO can use this system to confirm the user's status ("Active"), verify the correct Workforce Class assignment ("Affiliate Provider") has been applied, and display the KP Sponsor information (Name of System Administrator).

³ Starting in Q1 2022, user access provisioning will occur in AccessNow, the new consolidated platform for identity governance service.

3.9 KP HealthConnect Security

KP HealthConnect Security (<http://userprov.kp.org:8080/portal/html/NcalGenUser.jsp>) is the KPHC User Security Provisioning and Management portal by which the SA or KPBO can:

- Run a user access utility check (click Check User Utility, enter the user's NUID)
- Verify Epic account templates, security classes, user roles, and profiles

4. Post-Provisioning Guidance

4.1 How to Access Health Records

4.1.1 KP Online Affiliate

KPBO provides the [KP Affiliate Link General User Guide](#) to Affiliate users to help them navigate the KP Online Affiliate system. For Skilled Nursing Facilities, Home Health, and Hospice users, the KPBO provides the [KP Affiliate Link General User Guide for SNF-HH-HO Users](#).

NOTE: These user guides are proprietary, intended for internal use only, and must not be distributed outside of the Affiliate group.

When access to KP Online Affiliate (<https://epiclink-nc.kp.org/ncal/epiclink>) is granted, the Affiliate user signs on to KP Online Affiliate, where the user can view member and patient information by providing these four data elements:

- Member or patient name
- Date of birth
- Medical Record Number
- Gender

4.1.2 Epic Hyperspace

When access to Epic Hyperspace—the KPHC platform—is granted and the Regional Applications Portal is installed on the user’s desktop, the user can access a patient record by using the Search box and providing the search criteria, such as patient full or partial last name.

4.2 Access and Monitoring Reviews

4.2.1 CARMA Access Review

The Certification of Access and Role Management Application⁴ ([CARMA](#)) is a web-based tool that automates components of the User Access Review (UAR) process that is conducted periodically to ensure the continued need for the user access. It is the system used by managers to affirm that each user’s access is valid, appropriate, and required.

- Annual CARMA Review

Upon receipt of the CARMA list of Affiliate users, the SA collates the CARMA review list according to the designated KPBO and sends the list to the respective KPBO. The KPBO

⁴ Starting in Q1 2022, access review and recertification will occur in AccessNow, the new consolidated platform for identity governance service.

reviews the list to identify user access that should be retained and those that should be revoked. The KPBO then returns the list to the SA so the changes can be applied in CARMA.

- On Demand CARMA Review

Occasionally, when an Affiliate user registers in KP Online Affiliate, CARMA sends a request to the SA to confirm the user access to which the SA responds to confirm the request.

4.2.2 NCAL iACT Monitoring Review

On a monthly basis, NCAL iACT generates a monitoring report on Affiliate users which it sends directly to the KPBO. The KPBO examines the report for inappropriate access by Affiliate users. If a suspect activity is identified, the KPBO must notify NCAL iACT and the System Administrator. The SA will in turn inform the NCAL Area Compliance Officer, the NCAL Privacy and Security Officer, and any regulatory agency, as required, to initiate the prompt investigation of the issue.

Appendix A: NCAL Affiliate User Onboarding Checklist

NOTE: The Affiliate user onboarding activities below are listed in the sequence described in *Section 3: KPHC Access Provisioning Procedures* of this document. However, some activities may occur concurrently to ensure timely completion. This checklist may also be downloaded from [NCAL Affiliate User Onboarding Checklist](#).

Activity	Details	Reference	Date Submitted	Date Approved or Completed	Comments
Access Provisioning					
KPBO completes an <i>Access Request Form (ARF)</i>	KPBO completes and submits the <i>ARF</i> to NCAL-NKP-PRO@KP.ORG with copy to the respective NCAL Area Compliance Officer.	Access Request Form (ARF) <i>Refer to Appendix B: NCAL Area Compliance Officers for a list of ACOs</i>			
KPBO obtains all pertinent contracts and agreements from the Affiliate group	KPBO obtains a signed <i>KP Contractor Affiliate Web Sites License – Provider Entity Agreement</i> from the Affiliate group	KP Contractor Affiliate Web Sites License – Provider Entity Agreement			
	For Epic Hyperspace access, KPBO obtains the signed <i>KPHC Electronic Medical Record Access Agreement</i> from the Affiliate group	KPHC Electronic Medical Record Access Agreement			
	For Mental Health/Chemical Dependency health information access, KPBO obtains the signed <i>KP Contractor Affiliate Websites License MHSA</i> .	KP Contractor Affiliate Web Sites License MHSA			
	KPBO utilizes the <i>Business Associate Justification Log – Decision Tool</i> to determine if a BAA is required. If required,	Business Associate Justification Log – Decision Tool			

Activity	Details	Reference	Date Submitted	Date Approved or Completed	Comments
	KPBO obtains the signed <i>Business Associate Agreement</i>.	Business Associate Agreement Template			
	KPBO obtains a signed <i>Non-KP Provider Confidentiality Agreement</i> from each Affiliate user before access can be granted. This form applies to most users. For users who need access to Mental Health and Chemical Dependency records, a signed <i>Non- KP Provider Confidentiality Agreement MHCD</i> must be obtained from each Affiliate user.	Non-KP Provider Confidentiality Agreement Non- KP Provider Confidentiality Agreement MHCD			
	KPBO submits all signed documents to NCAL-NKP-PRO@KP.ORG				
KPBO completes the <i>Non-KP Access Monitoring Report Form</i>	KPBO completes and submits the applicable monitoring form to NCAL-RCO-iACT-Reporting@kp.org with a copy to NCAL-NKP-PRO@kp.org. If the NUID is not yet available, resubmit the form when the user receives their assigned NUID.	Non-KP Access Monitoring Report Form Non-KP Access Monitoring Report Form for SNF/HH/HO Users			
KPBO conducts the <i>Non-KP Affiliate User Training</i>	KPBO conducts the <i>Non-KP Affiliate User Training</i> which serves to familiarize Affiliate users with KP security and privacy policies and procedures including requirements for the safeguarding of protected health information (PHI).	Non-KP Affiliate User Training Template			

Activity	Details	Reference	Date Submitted	Date Approved or Completed	Comments
KPBO provides the KP Online Affiliate Registration Guides to the Affiliate group	KPBO provides the <i>KP Online Affiliate User Registration Guide</i> to the Affiliate group. The guide shows the Affiliate user how to self-register using the web-based NCAL Community Provider Portal (CPP) to obtain view the electronic medical records of Kaiser Permanente members. Each new Affiliate user must register.	KP Online Affiliate User Registration Guide Tips for the KP Business Owner (KPBO)			
	KPBO provides the <i>KP Affiliate Link Bulk User Registration Guide</i> to authorized Affiliate group managers and administrative staff with Administrator-Level Access to enable them to register multiple Affiliate users at a time using a downloadable spreadsheet.	KP Affiliate Link Bulk User Registration Guide Tips for the KP Business Owner (KPBO)			
SA reviews the KPIM-AP queue to approve or reject access	SA reviews the queue for provisionally registered KP Online Affiliate users who have requested clinical access. If the SA approves the request, a new NUID is assigned to the user and KP Online Affiliate Registration can be finalized. If the SA rejects the request, the user will need to address the issue.	KPIM-AP KPIM-AP Administrator Guide			
SA responds to CARMA request to approve user access, as needed	When an Affiliate user registers in KP Online Affiliate, occasionally a confirm request is systematically sent via CARMA to the SA. The SA responds to the request and confirms access.				
The SA or KPBO confirms the user's status,	The SA or KPBO confirms the user's status ("Active"), verify the correct Workforce Class assignment ("Affiliate Provider, and	KPIM			

Activity	Details	Reference	Date Submitted	Date Approved or Completed	Comments
Workforce Class, and KP Sponsor	display the KP Sponsor information (Name of System Administrator) in KPIM.				
SA or KPBO runs user access utility check and verifies account templates, security classes, user roles, and profiles	SA or KPBO runs a user access utility check (click Check User Utility, enter the user's NUID) and verifies Epic account templates, security classes, user roles, and profiles in KP HealthConnect Security.	KP HealthConnect Security			
KPBO provides the <i>KP Affiliate Link General User Guide</i> to Affiliate users	KPBO provides the <i>KP Affiliate Link General User Guide</i> to Affiliate users.	KP Affiliate Link General User Guide			
	KPBO provides the <i>KP Affiliate Link General User Guide for SNF-HH-HO Users</i> to Skilled Nursing Facility, Home Health, and Hospice users.	KP Affiliate Link General User Guide for SNF-HH-HO Users			
Access Maintenance					
KPBO reviews annual CARMA user access reports	Upon receipt of the annual CARMA report from the SA, the KPBO reviews the list to identify user access that should be retained and those that should be revoked. The KPBO then returns the list to the SA so the changes can be applied in CARMA.				
KPBO reviews monthly NCAL iACT monitoring reports	Upon receipt of the NCAL iACT monitoring report, KPBO reviews the report to examine for inappropriate access by Affiliate users and notifies the SA.				

Activity	Details	Reference	Date Submitted	Date Approved or Completed	Comments
SA deactivates Affiliate user who no longer require access	When notified by the KPBO that an Affiliate user no longer needs access, the SA revokes the access of the user and notifies NCAL-RCO-iACT-Reporting@kp.org .				
SA deactivates Affiliate group who no longer require access	When notified by the KPBO that an Affiliate group no longer needs access, the SA revokes the access of all Affiliate group users and notifies NCAL-RCO-iACT-Reporting@kp.org .				

Appendix B: NCAL Area Compliance Officers

Area	Compliance Officer	Contact Details
Hub 1 – Central Valley/Fresno	Patty Thompson	Patty.C.Thompson@kp.org (559) 448-3747 (559) 341-5703
Hub 2 – Diablo/Marin-Sonoma	Cris MacKenzie	Cristina.Mackenzie@kp.org (415) 893 4194 (415) 699 9355
Hub 3 – East Bay/GSAA	Richard Contreras	Richard.J.Contreras@kp.org (510) 752-7918 (408) 315-4499
Hub 4 – San Francisco/Redwood City	Deanne McCoy	Deanne.Mccoy@kp.org (209) 232-0911
Hub 5 – Roseville/Sacramento	Daphne Copenhaver	Daphne.X.Copenhaver@kp.org (916) 474-2032 (916) 755-2824
Hub 6 – Napa Solano/South Sacramento	Andrea Lenoir	Andrea.A.Lenoir@kp.org (707) 624-4253 (707) 227-7997
Hub 7 – San Jose/Santa Clara/Santa Cruz	Kathryn Pyke	Kathryn.S.Pyke@kp.org (408) 851-5344 (408) 318-3734
KPPACC ⁵	Margaret Chan	Margaret.Chan@kp.org (510) 847-6748

⁵ Kaiser Permanente Post-Acute Care Center (KPPACC) is a skilled nursing facility in San Leandro for patients that have been discharged from an acute care hospital but still need continuing treatment.

Appendix C: Contacts

Access Support

- Contact KP-NCAL-OnlineAffiliate (kp-ncal-onlineaffiliate@kp.org) for support on access issues

NCAL iACT

- Contact NCAL iACT (NCAL-RCO-iACT-Reporting@kp.org) for information on the NCAL iACT monitoring program.

KPIM and KPIM-AP

- Visit <https://kpim.kp.org/kpim-ap/secure> for information on KPIM-AP.
- Contact IAM IDM OPS-IREG (IAMIDMOPS@kp.org) for KPIM and KPIM-AP support.
- ASG DRTAS KPIM SUP – New System Administrators may request access to KPIM-AP by submitting a [Directed Service Request](#) in ServiceNow. Type in “Access”, then click “Select a support group”, enter “ASG DRTAS KPIM SUP”, and provide a detailed description of the request.

KPHC Security

- Stephen G Zirkelbach (Steve.Zirkelbach@kp.org), KPHC Web and Mobile Team: Affiliate Link – Responsible for the creation and modification of HealthConnect Security templates.
- KPHC CN AFFILIATE CD – System Administrators may request assistance from the KPHC Web and Mobile Team: Affiliate Link by submitting a [Directed Service Request](#) in ServiceNow. Type in “Access”, then click “Select a support group”, enter “KPHC CN AFFILIATE CD”, and provide a detailed description of the request.

Regional KPHC Security

- Contact NCAL-HealthConnect-Security (NCAL-HEALTHCONNECT-SECURITY@kp.org) for questions on Regional KPHC Security.
- KPHC CN SECURITY PROVISIONING CD – System Administrators may request assistance from Regional KPHC Security by submitting a [Directed Service Request](#) in ServiceNow. Type in “Access”, then click “Select a support group”, enter “KPHC CN SECURITY PROVISIONING CD”, and provide a detailed description of the request.

Appendix D: References

Affiliate User Onboarding Checklist

- [NCAL Affiliate User Onboarding Checklist](#)

Affiliate Access Templates

- [Affiliate Eligibility Access Template](#)
- [Affiliate Provider Read Only Access Template](#)
- [Non-KP Provider Read Only Access Template](#)
- [Non-KP Provider Read/Write Access Template](#)
- [Affiliate Provider Read Only MHCD Access Template](#)
- [Affiliate HHHO Access Template](#)
- [Affiliate SNF Access Template](#)
- [Affiliate Provider Surgery Center Staff Access Template](#)

License, Contract, and Agreement Templates

- [KP Contractor Affiliate Web Sites License – Provider Entity Agreement](#)
- [KPHC Electronic Medical Record Access Agreement](#)
- [KP Contractor Affiliate Web Sites License MHSA](#)
- [Business Associate Justification Log – Decision Tool](#)
- [Business Associate Agreement Template](#)
- [Non- KP Provider Confidentiality Agreement MHCD](#)

NCAL iACT Monitoring Forms

- [Non-KP Access Monitoring Report Form](#)
- [Non-KP Access Monitoring Report Form for SNF/HH/HO Users](#)

User Training Template

- [Non-KP Affiliate User Training Template](#)

KP Online Affiliate Registration Guides

- [*KP Online Affiliate User Registration Guide*](#)
- [*KP Online Affiliate Bulk User Registration Guide*](#)

KP Online Affiliate User Guides

- [*KP Affiliate Link General User Guide*](#)
- [*KP Affiliate Link General User Guide for SNF-HH-HO Users*](#)

KPBO Tools

- [*Tips for the KP Business Owner \(KPBO\)*](#)

KPIM-AP Tools

- [*KPIM-AP Administrator Guide*](#)

Document Revision History

Version No.	Date	Description of Change	Approved by
1.0	12/3/2021	Initial release	Yuan Chen, Executive Director, Privacy Compliance Angela Anderson, Director, NCAL Privacy and Security Officer