

Instructions

Read the Information Security and Confidentiality Policy. Failure to comply with policy may result in corrective action, up to and including immediate termination. Fax completed and signed forms to the IT Customer Support Center at 415-353-9025. All requests will be completed within 72 business hours of confirmation from the approving manager. Incomplete or unreadable requests cannot be processed and will delay account creation/changes.

A - Request Type

- New Account / Access
- Modify Existing Access
- Extend Existing Access

B - System Account Type

- Network (Standard Windows)
- Network for Rweb ONLY
- Network for SharePoint ONLY
- Telephone Authorization Code
- E-Mail - Section H
- IDX Flowcast - Section I
- SMS - Section J
- Picis - Section K
- Carecast - Section L
- TSO
- UGS/Ivans
- Ontrac
- Remedy
- Sentillion
- VPN (Remote Access) PC MAC
- Other _____
- Other _____
- Other _____

C - Employee Information

- Gender Male Female
- Employee (Full/Part time non-med)
- ID _____
- Medical Staff Credential Number
- ID _____

D - Vendor / Temp Information

- Consultant Temporary
- Vendor Other non-employee
- Account Expiration _____
- NOTE: The expiration date must not exceed 12 months. If no date is specified, access will be granted for 30 days.
- Company _____
- Address _____
- City _____
- State _____ Zip _____
- Supported Systems _____
- Signature _____

E - System User Information

- Last Name _____
- First Name _____
- Job Title _____
- Telephone Number Primary _____
- Telephone Number Alternate _____
- Building Location _____
- Department Name _____
- E-Mail _____

F - Approving Manager Information

- Last Name _____
- First Name _____
- Telephone Number Primary _____
- Telephone Number Alternate _____
- E-Mail _____
- Business Need _____
- Account Number _____ Fund _____
- Signature _____ Date _____

Account requests will not be processed until positive confirmation from the approving manager is received and verified.

G - Server Account Information

- Server Access (i.e., \\fpmcb11) _____
- Folder Access (i.e., \\fpmcb11\admin) Read Only Full Access _____
- Create Personal Share (P: Drive) Additional Permissions _____
- Same access as _____

H - E-Mail Account Information

- Distribution List Membership _____
- Additional Mailbox Access _____
- Same distribution lists as _____

I - IDX Flowcast Account Information

- Flowcast Profile or name of existing system user with desired access _____
- View Only PCS Access TES Access

J - SMS Account Information

- Name of current SMS user with desired access _____
- View Only Moffit Long Mount Zion

K - Picis Account Information

- Anesthesia Resident CRNA Neuromonitoring Tech RN Nurse Practitioner Surgeon Scrub Nurse Perfusionist
- Anesthesiologist Other Doctor Medical Student RN/FA Fellow Surgical Resident Surgical Tech
- _____ _____ _____

L - Carecast Account Information

- Attending Medical Student ED MD ED Nurse Pharmacy USC HIMS Support Personnel
- Resident ED Resident ED Clerk Nurse Ancillary Reg/ADT Info Desk
- _____ _____ _____
- Same access as _____

*** Access Control Use ONLY ***

- Processed by _____ Process Date _____ Change Request _____

A – Request Type

Check the appropriate box.

B – System Account Type

Check all Account Types you are requesting action on. If you are requesting “UCare” access, you need to check the “IDX Flowcast”, “Carecast”, and “Sentillion” boxes in Section B, and provide appropriate information in Sections I and L.

System Account Types not listed should be written in at the bottom under “Other”. Requests for VPN accounts include review and agreement with the “VPN Guidelines” below.

VPN Guidelines: *[VPN accounts for non-Medical Center employees will terminate on the contract end date unless department sponsor submits an Account Request form for account renewal.]*

- UCSF Medical Center VPN accounts are issued only to UCSF Medical Center physicians, employees or staff members. Requests for UCSF Medical Center VPN accounts require the approval of the employee’s department manager.
- Use of the UCSF Medical Center VPN account and the VPN Client Software is restricted to the employee, physician, or staff member whose signature appears on this form. No unauthorized users residing at the authorized user’s residence, place of business, or alternate work site are permitted to use the client software at any time.
- The authorized user is responsible for the safekeeping of the VPN Client software at all times. The authorized user must not distribute client software to any other person or persons.
- The authorized user is responsible for safeguarding active VPN connections; he/she must be physically present at the computer that has the VPN software installed whenever initiating VPN connections to the UCSF Medical Center network. Computers that have an active connection to the VPN switch must never be left unattended.
- The authorized user must disconnect an active VPN connection whenever he/she is not actively working on the computer or when the computer will be left unattended for any period of time.
- The authorized user is prohibited from downloading and/or distributing confidential PHI (Patient Health Information) to their personal PC or laptop.
- The authorized user is responsible for complying with the security guidelines and standards set forth in the existing UCSF Medical Center policies. This includes following the standards set forth for VPN access, changing your UCSF Medical Center network password every 60 days, downloading software updates or patches, complying with encryption and authentication methods, etc.
- The UCSF Medical Center IT department reserves the right to revoke the privileges of the VPN account at any given time subject to the guidelines set forth in this document.

Requestor’s Statement of Agreement: *I hereby request that a VPN Logon ID and Authorization Code be issued to me and I agree to use the VPN connection for business purposes only. I understand that I will only be able to access those systems for which I have an established logon ID and password. Furthermore, I agree to preserve the integrity of Protected Health Information (PHI) and other confidential data, by adhering to these Guidelines. I understand that if I violate any of the terms of this agreement, my VPN access may be revoked at any time and I may be subject to disciplinary action up to and including termination and criminal prosecution.*

Note to all Macintosh VPN users: *This VPN account is intended to provide you secure Telnet/SSH access to Medical Center critical business systems only. This account does not provide other services such as POP3, OSX server admin, Timbuktu, and Meeting Maker at this time.*

C – Employee Information

Employee ID (UCID) is **REQUIRED** for all employees. Non-employees **MUST** complete Section D.

D – Vendor/Temp Information

Consultants, vendors, temporary, or other non-employees **MUST** complete this Section. Employees **MUST** complete Section C. Account Expiration date may not exceed 12 months. If no date is specified, access will be granted for 30 days ONLY. This Section **MUST** include an authorized signature.

E – System User Information

This Section is **REQUIRED**. Only LEGAL names, not nicknames, should be entered in this Section.

F – Approval Manager Information

This Section is **REQUIRED**. Account Requests will not be processed until positive confirmation from the approving manager is received and verified.

***Account Request Form
Instructions***

G – Server Account Information

This Section needs to be completed if you are requesting a Network account.

H – E-Mail Account Information

This Section needs to be completed if you are requesting an E-Mail account.

I – IDX Flowcast Account Information

Complete this Section when requesting a new IDX Flowcast or “UCare” account or modifications/extensions to an existing account.

J – SMS Account Information

Complete this Section only when requesting a new SMS account or modifications/extensions to an existing account.

K – Picis Account Information

Complete this Section only when requesting a new Picis account or modifications/extensions to an existing account.

L – Carecast Account Information

Complete this Section when requesting a new Carecast or “UCare” account or modifications/extensions to an existing account.

**Please direct any questions regarding the Account Request Form to the
IT Customer Support Center at 514-4100, option 1.**