What is DUO?
DUO is a multi-factor authentication service that dramatically increases the organization's
security posture by adding something "you have" (a unique, one-time-PIN in this case) to your password (which can be guessed or cracked). Basically, any service with the added protective layer of DUO will require you to enter a numeric PIN (which is sent to your cell phone) after your password, and before you are granted access to that service or resource. With this in mind, you will need to have your mobile device with you whenever your login to a DUO secured resource or system.

Our project will focus on protecting our VPN systems, and at UCSF BCHO this means "Cisco Any Connect" - so, if you are a user of this system, you should anticipate some changes. We will begin the implementation with a pilot that is focused on key Accounting and HIS Department users.

The first step in the process is downloading the DUO app from the App Store[1] or Google Play[2].

Then, you will need to enroll your device[3].

Some key things to know about DUO ...

- DUO is a "cloud-based service" built and maintained by a leader in the information security space.
- When a resource is secured with DUO, multi-factor authentication is mandatory, not optional.
- DUO is the preferred multi-factor system at UCSF, and will eventually be used at BCHO for multiple services (not just VPN).

Pilot Timeline

The pilot program will commence in November 2017. DUO service will become IT supported before the calendar year ends.

Who can I contact for DUO training and/or technical assistance during the pilot?

During the pilot, you may contact Jacqui Larripa in HIS:

Email: JLarripa@mail.cho.org[4]
Phone: 510-428-3000 ext. 2280

For more information about this pilot, please contact:

IT Project Manager, Peter Robichau: hispro@mail.cho.org[5]

GET IT HELP. Contact the Service Desk online, or phone 415.514.4100