Duo Hardware Token Process for UCI Health Employees

Users (with email delivery point @hs.uci.edu) looking to use hardware tokens for both UCI and UCI Health should be given the following information.

1. Users will need to procure their own Yubi Key Tokens from the following site https://www.yubico.com/store/ and must purchase a Yubikey FIPS Series token. UCI Health will not process requests for Non FIPS Devices.

YubiKey FIPS Series

FIPS 140-2 Validation Ensures Strong Security and Compliance - The YubiKey FIPS Series enables government agencies and regulated industries to meet the highest authenticator assurance level 3 (AAL3) requirements from the new NIST SP800-63B guidance.

Once users has obtained their key they will need to open a service desk ticket to UCI Health – Data Security Team with the following information “Serial Number, Private Identity, and Secret Key”


Example:

01231337, 0c 87 99 55 78 ee, a4 d0 93 a9 bd 09 e1 24 e9 17 b6 72 03 56 a1 3b

OIT will hold configuration slot 1 of the Yubikey and UCI Health will hold configuration slot 2 to eliminate confusion if their keys need to be regenerated without affected exiting registrations.

How to get this information how to is available at the following site: https://duo.com/docs/yubikey
If the users is unable to generate keys they can drop off they keys with UCI Health desktop support team or arrange for a zoom meeting to step them through the key generation.