David Geffen School of Medicine

DGIT | Digital Technology

Reminder: Encrypt and Register Your Devices

In order to keep protected health information (PHI) and restricted information (RI) secure, all mobile devices and removable media used for University business must be encrypted and password protected, in compliance with HS Policy No. 9453-C.

What is happening?

We are doing a routine audit of our current list of registered encrypted devices, and we need your help to ensure that all laptops being used for University business are both encrypted and registered.

How will this affect me?

Encrypting your device protects any PHI/RI stored on the device and registering your device protects you by providing proof of encryption in case the device is lost or stolen. Inability to provide proof of encryption for lost/stolen devices could lead to fines and penalties for UCLA and personally for you.

If you have not already done so, you must encrypt your laptop, and register the encryption, before continuing to use it for University business. Additionally, laptops that are not encrypted will soon be blocked from accessing the Mednet network, both wirelessly and via VPN.

What do I need to do?

If you need to encrypt your device, check to ensure that it is encrypted, or register the encryption, please visit IT Connect and a support specialist will be happy to help you.

IT Connect

Location: Center for Health Sciences (CHS) building in the area west of Cafe Med
Hours: Monday - Thursday, 8 a.m. to 5 p.m.; Friday, 8 a.m. to 3 p.m. Closed holidays.

Questions?

If you have any further questions regarding the policy requirements for encryption of mobile devices, please contact the Office of Compliance Services or call Customer Care at (310) 267-CARE (x7-2273).