

E-Mail Use for UCDCM Personnel (Employees, Faculty, Staff, Volunteers and Students)

UC Davis Medical Center

Hospital Policies and Procedures

Policy ID: 1314

Revised 11/10/2015

I. PURPOSE

This policy mandates the use of only the University of California, Davis, Health System (UCDHS) official e-mail account for all UCDHS business related activities and provides alternative methods for sending secure information. At this time, the official UCDHS email system is Microsoft Office 365.

II. SETTING

Medical Center

III. POLICY

A. UCDHS Email Accounts

All UCDHS personnel (employees, faculty, staff, volunteer and students) must use the official Health System e-mail (currently Microsoft Office 365) for all work-related activities associated with UCDHS business. **Individuals shall not auto-forward their Microsoft Office 365 account to any other non-UCDHS e-mail account, including but not limited to, Gmail, Yahoo, Hotmail, etc.**

B. Encryption

Encryption is available for all UCDHS Microsoft Office 365 account holders and must be used when e-mailing PHI or PI to any non-UCDHS email accounts. To send email securely and encrypted to external recipients, include the following in either the subject line or body of the message: #secure#external recipients by including the term #secure# anywhere in the subject line or message content. This process will hold the message for the external recipient in an encrypted, secure system and send a proxy message. The proxy message will direct the external recipient to create a secure account on the encryption system. Once the account is created and the recipient confirms access, then the message can be retrieved only by the validated recipient.

This will send a proxy message to the recipient with a link to our secure encrypted email repository. The site will require the recipient to login with their credentials or a one-time pass code to retrieve the message. All replies and forwards of the encrypted message thread will be secured as well.

C. Alternative Methods of Sending Secured Messaging and Files

UCDCM personnel are strongly encouraged to use the following secure electronic communication methods:

1. **Secure Communication with Patients**

MyChart, the patient Personal Health Record (PHR), should be used when communicating with patients. For more details go to http://www.ucdmc.ucdavis.edu/medicalcenter/features/20100624_MyChart.html.

2. **Communication with Community Physicians**
PhysicianConnect should be used to share information about a patient with community physicians and their staff. This is a web based, view only module in Epic that allows users to view the UCD Electronic Medical Records of specified patients. This access method is encrypted and fully secured. Clinicians can request access to PhysicianConnect at <http://www.ucdmc.ucdavis.edu/referrals/>.
3. **Sharing Files with People or Organizations External to UCDHS**
Microsoft Office 365 OneDrive should be used for large attachments that cannot be sent via email. The OneDrive system is secure and recipients are sent an invitation when files are shared. This option can be used when sharing files with business partners or external entities. This option is accessed via Outlook Web Applications (OWA).

To request assistance with using OneDrive please contact the IT Operations Center at 734-HELP (4357).

A Secured File Transfer Protocol (SFTP) should be used for large attachments that cannot be sent via email. This option can be used when sharing files with business partners or external entities. This option is accessed via special software and a SFTP server.

To request access to SFTP please contact the Access Request Department by:
Phone: 734-HELP
Email: ISCS@ucdmc.ucdavis.edu
Online: <https://hsapp5.ucdmc.ucdavis.edu/gwisoft/help/sandars.nsf/>

Contact the IT operations center if you encounter issues with your SFTP account. The TOC can be accessed by:
Phone: 734-HELP
Email: ISCS@ucdmc.ucdavis.edu
Online: <https://ess.ucdmc.ucdavis.edu/src/secure/main.jsp>

REFERENCES:

UCDMC P&P 2442, Email Communication that Contains PI/PHI.
Civil Code Section 56.101
45 CFR Parts 160, 162, and 164 (HIPAA Security Rule)

Sent to the following for review:

Michael Minear
Scott Hebner*
Daniel Cotton
Anna Orłowski
Teresa Porter
Monte Ratzlaff
Stephen Chilcott
Health System Operations Compliance Committee