Department of Orthopaedic Surgery
Resident Computer and Email Policy

In an effort to comply with JACHO regulations, all email accounts for the orthopaedic surgery residents have been switched to the program Outlook and have been assigned a UCSD email address. **All UCSD communication will be sent to this email address in the future. You are responsible to check this email at least every other day. Not checking an email is not an excuse to miss information.** I will be sending out a list of the new email addresses to the faculty and staff. They will be instructed to send all their communication to that address from now on.

You may access your UCSD email at any computer that has access to the internet. The following are the instructions to access your new account. Please contact the Medical Center Help Desk if you have any problems accessing your email account.

COMPUTER PASSWORD GUIDELINES

Overview: The purpose of this guideline is to establish acceptable computing practices for passwords in the UCSD Medical Center, UCSD Medical Group, School of Medicine and School of Pharmacy environments. This guideline describes proper maintenance of password confidentiality, and emphasizes the importance of never sharing your password with someone else or with external service providers through re-use.

Scope: This guideline applies to anyone who has a password, administers passwords, or believes they have cause to share their own or someone else's password including faculty, fellows, nurses, staff, residents, trainees, students, research staff, and volunteers. This guideline applies to all systems which use passwords including: patient information system passwords, personnel system passwords, medical billing systems, desktop passwords, e-mail passwords, application passwords, private key passwords, etc.

Policy Statement: Each person accessing a computer system is personally responsible to secure and protect their password. You must never provide / divulge / share your password to or with anyone (including your supervisor or computer support personnel).

User Responsibilities & Procedures: The procedures can be summed up in one sentence:

Do not share your password with anyone or be in possession of anyone else's password.

Key Points:
1. Each authorized user must have their own UCSD login ID and password. It is a policy violation to share this login-ID /password.
2. HIPAA Security laws require that access to patient health information systems be limited to authorized users. Each individual who accesses patient electronic information systems requires their own access code and password.
3. Any actions (including unauthorized access) taken under a particular user ID will be attributed to the password's owner and misuse may result in disciplinary actions.

Tips:
1. Don't let your computer or Web browser "remember" passwords – anyone accessing the computer may be able to use your identity!

2. De-activate login-IDs when the user leaves a workstation / computer to prevent unauthorized access.
3. If someone asks you to let him or her use your account, just say no!
4. Employees may apply for computer access to UCSDMC's information systems by following the on-line application and authorization procedures on the Medical Center's Forms Management web-site:
    - http://forms.ucsd.edu
    - In the search term field enter the key words: "Information System".
    - Click "View File" to open the "Security Access Request Form" on-line; click to submit the request to the UCSDMC Security Team. Please allow up to 7 business days to set a new user up in the requested applications.

If someone is asking you for your password or is offering to give you their password, please simply decline. If you are pressured to share a password, notify the UCSD Medical Center Information Services Help Desk (619-543-7474), or call the UCSD Health Sciences Privacy Office (619-471-9150).

References:

✓ UCSD Medical Center Policy, MCP 210.1, "Security of Information Resources"
✓ UCSD Blink and search for "Information Security" policies, http://blink.ucsd.edu/