

# Protect confidential information, including all patient information.

---

## Your Account is only as secure as its password

- Don't let others watch you log in.
- Don't write your password on a post-it note.
- Don't attach it to your video monitor or under the keyboard.

### *Password Standard*

- Eight character minimum and should contain at least one of each of the following characters:
- Uppercase letters (A-Z)
- Lowercase letters (a-z)
- Numbers (0-9)
- Punctuation marks (!@#%&^\*()\_+=-)
- Some systems have limitations

### *Password Construction*

- It can't be obvious or exist in a dictionary.
- Every word in a dictionary can be tried within minutes.
- Don't use a password that has any obvious significance to you.

### *Password suggestions: Sentence*

- Pick a sentence that reminds you of the password. For example:
- If my car makes it through 2 semesters, I'll be lucky: imcmit2s,lbl
- Only Bill Gates could afford this \$70.00 textbook: oBGcat#7t
- Just what I need, another dumb thing to remember!: Jw1n,adtr!

### *Password suggestions: Vanity Plate*

- I feel great: if33lgr8!
- Dance of the red shoes: RED,\$hoes\$
- Dolphins Fan: d0lf1n'sfan

### *Password suggestions: Compound Words*

- Used every day and are easy to remember.
- Spice them up with numbers and special characters.
- Misspell one or both of the words and you'll get a great password.
- Friendship: Fr13nd+sh1p
- Lifelong: L!f3l0ng
- Lawnmower: lonm0-eR

## When sending confidential information by email

- For UCDHS uses, use Lotus Notes or RelayHealth
- Encrypt it if possible
- Confirm the recipient's address

## Should you open the e-mail attachment?

- If it's suspicious, don't open it!
- What is suspicious?
  - Not work-related
  - Attachments not expected
  - Attachments with a suspicious file extension (\*.exe, \*.vbs, \*.bin, \*.com, or \*.pif)
  - Web link
  - Unusual topic lines; "Your car?" "Oh! Nice Pic!" "Family Update!" "Very Funny!"

## Anything done under your login is your responsibility!

- Log off when you leave a workstation
- Do not share logins
- IS support can help when there is a problem logging in: don't log in for others' use
- Use auto logoff when possible

## Protect against viruses and worms

- Use a virus scanner and keep it updated
- Use a firewall when connecting to the internet
- Don't install unlicensed software
- Don't install something you are not sure of
- Be careful about what internet sites you visit

## Encrypt files on portable devices

- Laptops, PDAs, memory sticks.
- Laptop theft is our #1 risk!
- Soon, UCD will have an approved encryption solution.
- Better yet, avoid keeping ePHI and other confidential information on your portable device if at all possible.

## Wipe drives before getting rid of equipment

- Simple erasure is not enough.
- Darik's Boot and Nuke (<http://dban.sourceforge.net/>) is free and effective.

## Report security incidents / breaches

- Such as stolen computer; hacking

---

Report a security breach: UCDHS (916)734-8808 (after hours: (916)734-4357)

UCD abuse@ucdavis.edu or (530)757-5795

For technical assistance: UCDHS: (916)734-HELP; UCD: (530)754-HELP

Questions about the security rule: (916)734-8808