

CHG Computer Security Protocols

- **Passwords**
 - You may have one or two passwords that are used to access CHG data, a PC password which is used to log into the PC via gotomypc and a CHG Apps password, used to access the database programs, such as ClinApps, Marker, etc.
 - Your PC password must be different from your database passwords (and from any external accounts). Each password needs to be a minimum of six characters and a combination of upper case, lower case and non-letter characters
 - Passwords should not be stored on laptops in Outlook Express or any other applications nor taped to your monitor or around your computer
 - Passwords may not be shared with other people, nor may others use your account. They cannot be emailed unless encrypted.
 - Make sure you are aware of what you signed when you signed the Duke Confidentiality Form
 - Be aware, particularly in public places, that no one is watching you as you type your password
 - Per Duke policy, passwords must be changed every 180 days or the account will be locked.
- **E-mail communications**
 - Depending on your mail reader and location, your login and password information is encrypted when reading email but the contents of your email is *not*.
 - Do not open any suspect attachments regardless of the sender. New viruses can make the e-mail appear to be from anyone (including you) so you cannot trust the name of the sender.
 - If you think you have received a virus, contact your systems administrator.
- **Computer Security**
 - Keep the password screensaver turned on to the default setting (unless you choose to decrease the interval). If you leave your desk, you should manually lock your screen.
 - When printing sensitive information, pick it up from the printer immediately.
- **Personal Health Information (PHI)**
 - PHI information must not be stored on laptops, home computers, flash drives or local, non-networked drives. This includes information from CHG databases and hospital databases such as DHIS.
 - Emails sent outside Duke containing PHI must be encrypted. Contact your systems administrator for how best to do this.
 - To be HIPAA compliant, all media that contains any patient sensitive data must be disposed of properly. Give any CDs, diskettes, zip drives, etc that have contained patient data to your CHG contact who will give them to a CHG systems administrator to be erased.

Contact the CHG with any issues you may have or any of the following:

- Misuse of DUHS proprietary information, DUMC patient information, Duke employee information or CHG database information
- Unauthorized use of Duke systems in ways that compromise system availability, performance, or integrity.

CHG Password Policy

By choosing difficult passwords you ensure that in the event that our password file does get out, it is very unlikely that this will be of use to the hacker. This helps to maintain our high level of security, resulting in protection for the department at large. You **should not** use the same password on multiple accounts. Passwords must be at least six characters in length, a combination of upper case, lower case and non-alpha characters, cannot be the same as your previous ten passwords and must differ by at least three characters from your previous password. In addition, they should not be a word in any language forward or back. When you change your password, make sure there are changes made within the first eight characters. Passwords must be changed every 180 days.

Passwords that are easily guessed include the following:

- Dictionary words (of any kind: foreign, movie, Latin, obscure, high-tech), backwards or forwards

Hackers use several 10s of foreign dictionaries, movie dictionaries, or high-tech dictionaries in an attempt to guess passwords. Any word that might possibly be found in any dictionary is unsuitable.

- Any word that just has a number prepended or appended to it.
- Based on personal information

It is frequently very easy to guess a password that someone has chosen based on very little information about that person. It is sometimes possible to guess the password from information found on the web, if the chosen password is based on personal information. This includes name, department, birthday, anniversary, dog, cat, mother's maiden name, social security number, driver's license, etc... Therefore these passwords are unsuitable. Again, backwards or forwards are easily guessed.

Passwords that are acceptable include "random" strings, two words joined with selective replacement of key letters by punctuation, lyrics or verse joined in interesting ways, e.g.

random:	b4j/C5(*	
two words:	To@)fR0((toad frog)
lyrics or verse:	AtW*\$@w*	(All the world's a stage..)

Do not use any of the examples however, please come up with your own.