

Guidelines for Handling Confidential Information by Remote Access

You have signed an OHSU Confidentiality agreement as part of your employment responsibility. Please pay particular attention to sensitive information such as any data where the patient can be identified, confidential OHSU business data such as financial or strategic information, or information about employees at OHSU. In addition, if your job requires access to any patient information, you have also signed a Patient Confidentiality agreement. As stated in the agreement, if you look at information you are not authorized to access, or share it with others, this can lead to termination of your employment, loss of your clinical privileges, and removal of your access to OHSU electronic information and/or other sanctions. Remember, using remote access increases your responsibility since you are now effectively bringing OHSU electronic information outside of the OHSU facilities. When you are utilizing remote access, you must provide the same level of security used when working at an OHSU site. The following are suggested general guidelines to help you in that effort.

Passwords:

- Do not share your passwords
- Do not write down your passwords
- Do not use “save password” functionality and always type in the password
- Change your passwords often
- Conventions for choosing a password
 - Avoid passwords that are easy to guess such as names of pets, children, spouse, birth dates, addresses, or any words in a dictionary or thesaurus
 - Passwords attributes:
 - 8 character minimum
 - Inclusion of all of the following elements:
 - An alpha character (e.g. zyxwvut)
 - A numeric character (e.g. 12345); and,
 - A capitalized letter or punctuation or non-alphanumeric character (e.g. !@#*+)
 - Avoid words found in any dictionary (including medical, foreign language)
 - Shall not contain the user login-name (UserID)
 - For example, passwords constructed from the first letter of words from the title of a favorite song are easy to remember and difficult to guess
 - Another choice is a “phrase key” password (Don't Just Sit There! Do Something. Password: DJST!DS) for security reasons please do not use this example.

Paper:

- Only print something if you need a hard copy
- Make sure print outs are secured
- Destroy (shred or burn) printed material when it is no longer needed

Electronic Media:

- Only access data you are authorized to access
- Store diskettes, backup tapes and other electronic media in a locked cabinet/safe
- Completely wipe the data from diskettes, tapes and CD's before discarding or reusing. Note: Simple delete or reformat functions do not adequately eliminate electronic data. Determine where your applications store their temporary files, and examine these areas on a regular basis to make sure they do not contain any confidential information.

Physical Security:

- Be aware of your environment:
 - Who can see your screen when you are working on the computer
 - Who has access to your computer and/or files
- Password protect files
- Power-on password for computer
- Use a password on your screen saver activated after a short time out
- Logout of applications when you are finished
- Logout when you are going to leave the computer unattended
- Any loss or suspected burglary of equipment or software containing or used to access confidential OHSU information should be reported to OHSU Public Safety (4-7744) and the OHSU Integrity Office (4-8849).

Revised 8/3/2010 rgm