

CONFIDENTIALITY WITH CLIENT RECORDS – PASSWORD PROTECTION

We may exchange client information via email and attachments in an effort to move our work forward. Email allows us to quickly share information. We must make every effort to ensure that the exchange of information is secure to protect PHI. Please observe the following:

- Only use your UW email account to exchange documents regarding clients or subjects.
- If it is necessary to identify a client in an email (cancelled appointment, change in schedule etc.), use INITIALS ONLY. You can identify the supervisor, the day of the appointment, the unit (i.e., neuro, voice, etc.), but do not use the client's first and/or last name in email communication.
- If you communicate directly with a client or client's family/guardian via email, use your UW email account. We have internal security via the UW servers. DO NOT use your personal email outside of your UW account (i.e., AOL, Yahoo, etc.).
- If client documents (i.e., evaluation report, final case summary, cover letters, etc.) are being sent back and forth via email for Student/Supervisor editing or review, the documents must be "password protected" and must have PHI deleted until the final printing. In other words, you must not include full name, address, phone number until the final printing.

Password protecting documents:

Here's how you can password protect a document using WORD on a PC or MAC. Follow these guidelines:

1. Open the document (this is the report or cover letter you've just written)
2. On the File menu, click Save As.
3. On the Tools menu in the Save As dialog box, click General Options.
4. In the Password to Open box, type a password*, and then click OK.
5. In the Reenter Password to Open box, type the password again, and then click OK.
6. Click Save.

* Arrange with your clinical supervisor to have a "shared password".

From "Word's Help facility": A password can contain any combination of letters, numerals, spaces, and symbols, and it can be up to 15 characters long. Passwords are case-sensitive, so if you vary the capitalization when you assign the password, users must type the same capitalization when they enter the password. When you create a password, write it down and keep it in a secure place. If you lose the password, you cannot open or gain access to the password-protected document.