The following are provided as suggestions for protecting files. There may be alternative means by which you elect to secure files that you transmit. However, in the case of Practice Samples, all files that may contain Personal Health Information or other confidential information should be secured using encryption and a password/key for unencrypting the file. You may also have files that you want to "shred" at some point. Suggestions for that activity are also provided herein.

How to protect your files – caveat to Mac users your different mileage may vary….

Increased use of electronic files for practice samples and other materials that may include sensitive information makes an awareness of how to protect that information essential. There are many ways to protect the files and many of them are not at all difficult.

Step 1. Use up-to-date programs. If your programs are not the most recent, or at least recent enough to include file protection schemes, it is probably time that you upgrade and/or update.

Microsoft Office Products

Recent Microsoft Office programs (Word, Excel, PowerPoint, etc) all include very simple password protection and encryption schemes.

Open your document

Click on File in the upper left corner

Click on Info

Click on Protect Document

You will see a variety of choices, each of which is one type of document protection. You can select more than one of these and may wish to do so at times; however, for the purposes of encryption and password protection.

Click on Encrypt with Password

You will be prompted to type in a password. Make it difficult, but also one that you can either remember or store separately (perhaps in another encrypted, password protected file).

Save the document.

Using Pages on a Mac

Click on Manage Document, the select Password-Protect a document

PDFs using Adobe Acrobat Pro

Adobe provides directions here

https://helpx.adobe.com/acrobat/using/securing-pdfs-passwords.html

An alternate way from that described by Adobe is to open your pdf file, click on File, then click on Properties, then click on the tab marked Security and you will see a way to enter a password. As you do that, you will be given an option to encrypt the file (look a bit below the password entry spot) and other

options for user privileges. The encryption and password will not take place until you save the file, so be sure to do that once again after enabling the protection.

Videos –

Videos are just like any other file in many ways – except they tend to be much, much larger. One simple way to encrypt and password protect a video file is to insert the video into PowerPoint and then use the built-in protection in PowerPoint. In order to successfully transmit video files, especially through email, you may need to compress the file using a "ZIP" format or similar file compression scheme. Windows has the capability to compress a file built in. To access that, right click on the file and then select Send To, then select ZIP Folder.

Another way to protect your documents is to use a Utility Program that includes encryption and password capabilities. One such free program is Glary Utilities from GlarySoft (www.glarysoft.com). There are many such programs and searching sites such as www.download.com or www.filehippo.com will turn up several. If you go to these sites you could search for encryption, utilities, of use other terms.

Paid options also exist. PKWARE (www.pkware.com) was the originator of what many call a ZIP file. The program that compresses files into smaller sizes has been enhanced to include encryption (https://www.pkware.com/zip-solutions). The file compression software (PKZip) alone (no encryption) is $29 and the encryption/compression program (SecureZip) costs $39. You need only the $39 version to do both.

With any of the options that you look into, read about what tools, if any, those that you send your file to may need. They may merely need to know the password; however, some programs will require that your recipient also have a copy of that program.

Once you have protected your file, you may then send the document to others safely. Send them the password that they will need to open the file, but ***DO NOT*** send it in the same email or transmission as the file itself. Doing so would provide the password AND the file to someone should an unauthorized user access that email.

Finally, file destruction –

You may at some point want or need to dispose of an electronic file. Again, there are very good, free utilities that can assist in this. CCleaner (available from www.piriform.com) has a way of doing this, as well as a means of helping to keep your computer free from nagging adware and other files that can slow it down. You can use CCleaner on computers to assist in keeping the computer running smoothly.

For file destruction, Eraser is a good, free program (https://eraser.heidi.ie/download/) that is excellent and will give you numerous choices as to how to successfully delete a file. Most of these programs use the method of "over-writing" the file multiple times (the more often it overwrites the file, the longer it takes, but the more securely deleted – or shredded – the file becomes.). Using Eraser for this purpose simply requires a right click on the file name to open a menu to start the destruction process.