

Interoffice Memorandum

To:

From: Vince Temples, Privacy Officer

Re: Password Protection of Word Documents

Date: August 31, 2004

.....

Background

The Harris County Hospital District does not currently have a mechanism to encrypt e-mail. The HIPAA Security rule designates encryption as the preferred method of securing e-mails that contain patient information from unauthorized access. E-mail can be sent from addresses in the District (those addresses ending in @hchd.tmc.edu) to other addresses in the District or to Baylor College of Medicine addresses (those ending in @bmc.tmc.edu) or to the University of Texas (those addresses ending in @uth.tmc.edu) without going to the Internet. These e-mails are considered secure from access by persons outside the network and patient information may be included in these e-mails.

If e-mail is sent to other addresses, it will go over the Internet and be subject to possible access by unauthorized persons. **Patient information should NOT be sent in emails that travel over the Internet.**

When sending patient information by e-mail over the Internet, rather than entering the information into the e-mail, create a Word document containing the information. When the document is complete, protect the document with a password that must be entered before the document can be opened. The document can then be attached to an e-mail and sent either within the HCHD network or over the internet. The method for assigning a password to a Word document depends on the version of Word being used.

Password Protection Using Word 2000 or Word 2002

If you are using Word 2000 or 2002, open the document you wish to protect and click on Tools at the top of the screen (see the diagram below this paragraph). From the drop-down box, select Options. In Options click on the tab labeled Save. A drop-down box appears containing a box labeled "Password to Open" near the bottom. Click on the box and type the password you wish to assign to the document. Click OK. Reenter the password in the box that appears and then click OK again. Save and close the document and it can then be attached to an e-mail and sent to the intended recipient.

Tools → Options → Save → Password to Open → OK → Reenter Password → OK → Save

Notes:

- 1) **Be sure to provide the password to the recipient in a separate communication (fax, phone, etc.). Do not send the password in e-mail.**
- 2) If you are producing many of these documents, don't save the password protected versions on your computer (save it without the password). There will soon be too many passwords to track. You can delete the password from a particular document by following the steps above and deleting the password from the "Password to Open" box.
- 3) When you click on Tools, you will see in the drop-down box a selection called Protect Document. This function allows you to protect all or part of the document from being edited, **but it does not prevent the document from being opened and read.** Do not use this function to password protect a document containing patient information.

Password Protection Using Word 2003

In Word 2003 with the document open, click on Tools at the top of the screen (see the diagram below this paragraph). In the drop-down box, select Options. In Options click on the tab labeled Security. A drop-down box appears containing a box labeled "Password to Open" near the top. Click on the box and type the password you wish to assign to the document. Click OK. Reenter the password in the box that appears and then click OK again. Save and close the document and it can then be attached to an e-mail and sent to the intended recipient.

Tools → Options → Security → Password to Open → OK → Reenter Password → OK → Save

Notes:

See the Notes above.

Alternative Mechanisms for Conveying Routine Files

The methods described above will adequately protect information sent infrequently and non-repetitively. If you have a file that must be conveyed on a regular, recurring basis contact Dana Williams, IT Security, Harris County Hospital District at 713-566-6202. She will assist in determining if your files can be sent routinely as an automated transaction.