Securing Protected Health Information

Expectations of safely sending PHI outside of your organization:

- ✓ If agency's have the ability to send emails encrypted, this should be the first option because this is a more secure way of safely sending PHI.
- ✓ If your agency does not have the ability to send encrypted emails, you may send PHI through a password protected document.
- ✓ If you use the password protected method, the name on the file should not include PHI (including full names, DCNs, or even last names).
- ✓ When password protecting the document, you must send the password to the document in a separate email.

What's the difference between sending PHI through encrypted email and via password protection?

- ✓ Sending through an encrypted email forces the recipient to use a password to open the email itself.
- ✓ Sending an (non-encrypted) email with a document that is password protected forces the recipient to open the document using a password. Therefore if the email is "hacked," the "hacker" can access all of the information (including the title of the document) except what is directly inside the document.

Frequently Asked Questions:

Q: ***If I send an enrollment form in which the title has PHI through an encrypted email, do I have to password protect the document?***

A: No, because the email itself will be encrypted.

Q: ***How do I know if I can send an encrypted email?***

A: You need to talk with your IT staff to determine if you do. It is a misconception to think you can simply put [encrypt] in an email and this means the document is encrypted. This is only possible if your agency has his encryption server set up this way. There are numerous encryption servers and each may work a different way, so you must check with your IT staff if you are unsure.