Guidelines for Using Electronic Communication for Sharing Case Specific Information

All staff must be aware of the need to protect case specific information that identifies clients and the types of services being provided. Legal standards exist that limit re-disclosure of client identifiable information between and among district staff, contracted agency service providers or other persons who have a legal right to the information. The applicable standards depend on various factors, including the service type or other case factors such as whether it is HIV related information.

To maintain the confidentiality of case and individual client information, a staff person must use the following sequence of options for sharing data:

CONNECTIONS or other HSEN Application

Use the CONNECTIONS electronic case record to allow access to the information through a To Do or the assignment of a role; the CONNECTIONS system is the most secure method of sharing data and should be used whenever possible.

If it is information that is within any HSEN application that requires user authentication, then the application should be used to share information if possible.

If CONNECTIONS or the other HSEN application cannot be utilized, the user must then consider if there is another secure method that can be used to share the information. Can it be mailed via a surface carrier, can the other staff person be called, or can the material be hand delivered?

If none of the above alternatives can be used to share the information due to system or time constraints, the following options may be considered:

Shared Drive

Using a shared drive or SharePoint site to share information allows any computer connected to a network to potentially access the drive or site. With appropriate access and permissions set, it is a preferred way to share confidential information. Access to a drive where confidential information is stored must be monitored and routinely maintained in order to safeguard and preserve the integrity of the stored information.

Faxing When faxing confidential or case specific information, always alert the person to whom the data is being sent before it is faxed, verify the fax number and confirm that the information was received by that individual. Always use a cover sheet.

Electronic Mail If it is determined there is no alternative method of communicating the information and you must use email, then you must password protect the confidential information that you are sending. Please note that the email system within the intranet is secure, but there are still risks with using email outside of an HSEN application. Users must exercise caution. **The biggest risk in using any email system is user error (for example, inadvertently sending to the wrong person). If you are connected and have access to the OCFS network then you must use that email system. Do not use systems like MSN or AOL to send confidential information.** **Email should include the confidentiality transmission message.**

To Password Protect a Document:

If case specific information must be sent, put it in a WORD document or EXCEL spreadsheet and password protect it. There is more than one method to password protect. The directions below apply to MS 2003/ 2007 and Excel.

To **password protect a document**:

To password protect a WORD document or EXCEL spreadsheet that you are saving and sending:

Please note that if you forget the password, you cannot open or gain access to the password-protected document. (The owner can remove password protection.)

- Open the document
- On the **File** menu or MS Office Button , click **Save As**
- In the **Save As** dialog box, select **Tools** menu (top right or bottom left) click **Security Options, (General Options for Excel and MS 2007)**
- In the **Security** dialog box (**Save Options** dialog box for Excel) under file encryption options for this document, (file sharing for Excel), in the **Password to open** box, type a password, and then click **OK**
- In the Confirm Password dialogue box, in the **Re-enter password to open** (**Re-enter password to proceed** for Excel) box, type the password again, and then click **OK**.

- Click **Save**
- Call the person to whom you are sending the document and give him or her the password
- **Email the password protected document or spread sheet**

DO NOT REFERENCE THE INDIVIDUAL'S OR CASE NAMES IN THE SUBJECT LINE IN THE EMAIL.

Before hitting the Send button, be certain that the name of the person you have chosen is correct. There are many people in the Global Address Book with the same or similar names. This heightens the risk of sending information to the wrong person. If you are not sure of the identity of the person in the Global Address Book, right click on the name and then on Properties. If you are still unsure, call the person first to verify their email address.

Caution the person(s) to whom the data is being sent that the data is not to be forwarded without consideration of all of the issues contained in these guidelines.