WIC Electronic Record Checklist

Your Local Agency Procedure **must** include the following components.

**Scanner review and inspection plan that includes:**

[ ]  Who will inspect the scanner to ensure it is working properly;

[ ]  How often the scanner will be inspected;

[ ]  How the scanner will be inspected to ensure it is functioning properly;

[ ]  Who will ensure the scanned documents are readable and good quality;

[ ]  How the electronic files will be inspected to ensure they are readable and good quality (e.g. review a certain number of electronic files or scanned documents after scanning them);

[ ]  How the inspection of the scanner will be documented (e.g. see the sample form that staff can fill out when they do the inspection)

# **Sample inspection form**

Staff Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date of Inspection: \_\_\_\_/\_\_\_\_/\_\_\_\_\_\_\_\_\_

[ ]  Scanner is functioning properly? Yes \_\_\_\_ No\_\_\_\_

[ ]  Number of scanned files reviewed to ensure its scanning properly: \_\_\_\_\_\_\_

[ ]  Type(s) of scanned documents reviewed:

1. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
2. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
3. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
4. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

[ ]  Scanned files are good quality and readable? Yes \_\_\_\_ No\_\_\_\_

**Security plan including:**

[ ]  Physical location of main electronic files (computer or hard drive location, location on computer or hard drive, etc.);

[ ]  How access to the electronic files will be granted and who will have access to the electronic files;

[ ]  How access to the electronic files will be granted to ensure protection of confidential applicant and participant information;

[ ]  How you will keep the electronic files secure (e.g. password protection, encryption, limited personnel access);

[ ]  How you plan on organizing and naming the electronic files, so they can be easily identified and accessed.

**Backup and Recovery plan:**

[ ]  Where will the offsite storage of back-up files be located (e.g. cannot be the same location where they are regularly accessed);

[ ]  How will the files be protected (e.g. Offsite storage location fire suppression system/sprinklers, password protection, lock and key);

[ ]  What type of fire-resistant structure the backup electronic files are stored in. (e.g. fire proof safe or cabinet)

[ ]  How often will you save a new backup copy of all files.

[ ]  How you will recover the electronic files if the main electronic files are destroyed and the files are lost (e.g. fire, flood).