KRA CORPORATION
Innovative Exceptional Trusted

Standard Operating Procedure

Subject: Participant File Standards	Effective Date: October 2015
Responsibility: Corporate QA	Revision Date: March 2019
To: Program Managers	SOP No.: QA-001

Purpose:

To define company policy regarding participant file maintenance, inventory, and security, and to define KRA minimum standards as they pertain to each aforementioned topic. This SOP pertains to all programs that maintain hard copy files for program participants.

Background:

Participant case files are required to document programmatic requirements, activities, and outcomes of a customer's time in the program. Programmatic requirements include, but are not limited to, eligibility or enrollment documents. Documentation of activities may include training vouchers, work experience assignment, timesheets, or other documents that demonstrate participation. Outcomes may include credentials, certifications, or employment verification. While this list is not comprehensive and each program has unique requirements, it is imperative that each program maintain all necessary documentation to validate each participant and his/her activities. It is also essential that each program has appropriate standards for file maintenance, inventory, and security.

Procedure:

File Maintenance
All participant files should be organized and easy to follow. All documents should be completed in their entirety and easy to locate in the file.

It is KRA's policy that files are maintained according to a file checklist. The checklist can be a single sheet of paper, located either on the cover of the participant file or the first page in the file. For files that have multiple tabs, the program may choose to have a checklist for each tab. The checklist must list all applicable documentation that is to be filed in each section of the file, and indicate which of the documents are actually placed in the section with a check or mark on the checklist.

All documentation should be filed in the order specified by the checklist. This will allow for efficient and effective file reviews conducted by the program or other monitoring entities.

Each program has its own unique requirements. Therefore, KRA does not mandate any one method of maintaining organized files on each participant, except that files must provide a complete and accurate record of the customer's program participation, and that all required documentation is easy to locate.

Furthermore, we are in the business of obtaining meaningful employment for our customers. This cannot be done with a resume. It is KRA's policy that all customers have a resume within 90 days of being enrolled on one of programs.

Inventory
It is not acceptable to lose a customer's file.

To ensure files are not lost, all KRA programs are required to implement a file inventory procedure, and maintain a master list of all case files.

It is KRA's policy that 100% file inventory be completed on a quarterly basis, and include all active and exited files that KRA has responsibility for since the inception of the program. Files that are archived can be maintained in lockable storage containers or sealed in boxes with a list of participant files available for inventory attached, as applicable. Provided the files have not been accessed since the last inventory, the actual files do not need to be checked every quarter.

Case management personnel (Career Agents, etc.) should inventory their specific caseloads on a regular basis. The frequency of the case manager's inventory should be determined by the Program Manager based on caseload size and frequency of customer interaction.

The results of each inventory, including any missing files, are to be reported to the Corporate Quality Assurance Manager each quarter when the inventory is complete. Inventory results will be due on the last work day of March, June, September, and December of each year.

Should any files be missing, a corrective action plan (CAP) must be submitted along with the inventory results, and must include the steps the program will take to mitigate the chance of any future occurrence.

Security
While security is certainly related to file maintenance and inventory, protecting customers' Personally Identifiable Information (PII) and documents covered by the Health Insurance Portability and Accountability Act (HIPAA) is arguably the most important task we undertake from day-to-day. From the perspective of protecting KRA, our clients, our file management programs, and individual staff, the loss of PII resulting in identity theft or other fraud would be

catastrophic. Anyone can be named in a lawsuit should a customer choose to file one. It is with this understanding that we must place file security as a primary objective in everything we do. It is also a key factor in providing KRA's exceptional customer service.

PII is information that can be used on its own or with other information to identify, contact, or locate an individual. PII includes, but is not limited to: full name if not common, Social Security Number, mailing address, phone number, driver's license number, date and place of birth, etc.

HIPAA-protected documents include any materials that contain "individually identifiable health information" held or transmitted by a covered entity, in any form or media, whether electronic, paper, or oral. The HIPAA Privacy Rule published by the U.S. Department of Health and Human Services calls this information "protected health information" (PHI) that is individually identifiable and includes demographic data that relates to:
- the individual's past, present, or future physical or mental health or condition,
- the provision of health care to the individual, or
- the past, present, or future payment for the provision of health care to the individual,

and that identifies the individual, or for which there is a reasonable basis to believe can be used to identify the individual. Individually identifiable health information includes many common PII related identifiers (e.g. name, address, birth date, Social Security Number).

Regarding customer file security, KRA requires the following:
1. Do not use the SSN on documents except when required by the client.
2. All files must be maintained in locked storage containers when not in use.
3. No files are to be left unattended at any time unless secured in a locked cabinet or drawer.
4. No files are to be removed from the premises without being signed for by the individual transporting them.
5. Files transferred to another entity (e.g. the client for monitoring) must be signed for by the receiving entity and by a KRA staff member upon their return.
6. Documentation of all file transfers must be maintained by the program.
7. No files are to be taken home by any KRA staff member. This includes copies of documents containing PII or PHI.
8. All documents containing PII should be filed in the customer's file immediately. If the program utilizes an electronic file system, the documents should be scanned immediately and the original should be completely destroyed by cross-cut shredding machines (or other equally effective destruction methods) such that the results are not readable or useable for any purpose.
9. Information legally protected under HIPAA must be kept in a separate file that is locked and maintained by the Program Manager or his/her designee.
10. Abide by all contractual, client-specific requirements, which may be more restrictive.

Program Level Monthly Review and Report

At a minimum, programs are required to conduct monthly reviews of a sampling of programmatic files. File reviews are required to be submitted to the Corporate Quality Assurance Specialist or respective designee on the last work day of every month.

The sampling methodology should ensure that all customer categories can be selected, and that the selection methodology and sample size be submitted to, and approved by, the Corporate Quality Assurance Manager.

KRA's File Review and Report tool is available in the E-cabinet to assist in the review process. Complete instructions on how to use the tool are located on the second tab.

Refer any questions regarding this SOP to the Corporate Quality Assurance Manager.

<div align="center">*   *   *</div>