KRA CORPORATION Innovative Exceptional Trusted

Standard Operating Procedure

Subject: Protecting PII and PHI	Effective Date: October 2015
Responsibility: Corporate QA	Revision Date: March 2019
To: Program Managers	SOP No.: QA-004

Purpose:
To protect KRA's employees, career-and business-services customers, clients, and community associates and partners from the accidental release of protected information.

References:
- Training and Employment Guidance Letter (TEGL) 39-11 – DOL Guidance for Protecting PII
- 20 CFR 683.220 – WIOA Requirements for PII
- US DHHS – Summary of HIPAA Privacy Rule
- 45 CFR Parts 160 & 164 – DHHS Standards for Privacy of Individually Identifiable Health Information

Background:
The Privacy Act of 1974 and the Health Insurance Portability and Accountability Act of 1996 (HIPAA) require the safeguarding of certain protected information.

Personally Identifiable Information (PII)

The following definitions were taken directly from TEGL 39-11 published by the US Department of Labor (DOL)**:**

PII – The Office of Management and Budget defines PII as information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual.

Sensitive Information – Any unclassified information whose loss, misuse, or unauthorized access to or modification of could adversely affect the interests or the conduct of Federal programs, or the privacy to which individuals are entitled to under the Privacy Act.

Protected PII and non-sensitive PII – DOL has defined two types of PII, protected PII and non-sensitive PII. The differences between protected PII and non-sensitive PII are based primarily on an analysis regarding the "risk of harm" that could result from the release of the PII.

- Protected PII is information that if disclosed could result in harm to the individual whose name or identity is linked to that information. Examples of protected PII include, but are not limited to, social security numbers (SSN), credit card numbers, bank account numbers, home telephone numbers, ages, birthdates, marital status, spouse names, educational history, biometric identifiers (fingerprints, voiceprints, iris scans, etc.), medical history, financial information and computer passwords.

- Non-Sensitive PII, on the other hand, is information that, if disclosed by itself, could not reasonable be expected to result in personal harm. Essentially, it is stand-alone information that is not linked or closely associated with any protected or unprotected PII. Examples of non-sensitive PII include information such as first and last names, e-mail addresses, business addresses, business telephone numbers, general education credentials, gender, or race. However, depending on the circumstances, a combination of these items could potentially be categorized as protected or sensitive PII.

To illustrate the connection between non-sensitive PII and protected PII, the disclosure of a name, business e-mail address, or business address most likely will not result in a high degree of harm to an individual. However, a name linked to an SSN, a date of birth, and mother's maiden name could result in identity theft. This demonstrates why protecting the information of our program participants is so important.

Personal Health Information (PHI)

The US Department of Health and Human Services (DHHS) states that the Privacy Rule protects all "individually identifiable health information" held or transmitted by a covered entity, in any form or media, whether electronic, paper, or oral. The Privacy Rule 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, SSN, etc.)

In the simplest of terms, PHI is PII linked to the above medical descriptions and as such is afforded additional layers of protection by HIPAA.

Procedure:
KRA requires that all PII and PHI be protected in accordance with applicable laws, regulations, and guidance, as provided by the DOL, State regulations, and client requirements.

It is our legal requirement to protect this information. Every day, we are entrusted with protected information, and we must understand that failure to act in accordance with DOL guidelines can lead to civil and criminal sanctions for non-compliance. Information security is everyone's responsibility.

KRA requires that staff members adhere to the following procedures:

1. Limit collection and use of PII and PHI to the fullest extent possible to fulfill the contractual requirements.
2. Ensure that workstations are protected with strong passwords, which can include:
    a. At least one uppercase letter
    b. At least one lowercase letter
    c. At least one number, and
    d. At least one special character such as #, @, or %.
    e. Passwords should not include common names or dates.
3. Shred all unnecessary documents. Unnecessary documents 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.
4. Label folders or media that contain PII or PHI.
5. Password protect electronic files that contain PII or PHI or store them on an encrypted server such as KRA's E-Cabinet.
6. Do not save electronic PII on shared drives/folders or applications that do not have controlled access.
7. Be aware of your surroundings when discussing PII or PHI.
8. Do not leave out any documents or electronic media that contain PII or PHI when you leave your workspace, and lock it up at the end of the day.
9. Do not e-mail unencrypted PII or PHI. If you are not sure, do not send it.
10. Do not take PII or PHI documents home with you.
11. Do not share PII or PHI with anyone who does not have the need for it, or who has not been trained in how to protect it.
12. Never send electronic PII and PHI via unencrypted e-mail off an encrypted server (e.g. anyone@kra.com to anyone@notkra.com).
13. Electronic PII and PHI can be sent within the same encrypted server (e.g. someone@kra.com to someoneselse@kra.com).
14. Limit the collection and use of PII and PHI to the fullest extent possible to fulfill the contractual requirements. (Yes, this requirement is listed twice; it is that important!)

The Work Number

The Work Number is a means that KRA uses to determine the employment status of participants who have exited the various program we operate. While this is a vital tool used to validate performance, it requires certain personal information in order to function. The following guidelines are to be followed by all personnel with access to The Work Number.

Authorized Users must:

1. Not order The Work Number Data for personal reasons or provide Data to any third party except as required by your project.
2. Be aware that unauthorized access to The Work Number Data may subject them to civil and criminal liability under the FCRA punishable by fines and imprisonment.
3. Ensure that all devices used to order or access The Work Number are:
    a. placed in a secure location, and
    b. are accessible only by them, and
    c. that such devices are secured when not in use through such means as screen locks, shutting power controls off, or other security procedures and controls which are standard practice in the data protection industry.
4. Never share their The Work Number user ID or password with anyone.
5. Change their KRA network passwords at least every 90 days, or sooner if it suspects an unauthorized person has learned an Authorized User's password.
6. Never, under any circumstance, access The Work Number via any unsecured wireless hand-held communication device, including but not limited to, web enabled cell phones, interactive wireless pagers, personal digital assistants (PDAs), mobile data terminals and portable data terminals.
7. Never, under any circumstance, use non-work related assets such as personal computer hard drives or portable and/or removable data storage equipment or media (including but not limited to laptops, zip drives, tapes, disks, CDs, and DVDs) to store the Data.
8. Ensure data are encrypted when not in use.
9. Ensure, if they must transfer or ship any Data, they encrypt the Data using the following minimum standards, which standards may be modified from time to time by EVS: Advanced Encryption Standard (AES), minimum 128-bit key or Triple Data Encryption Standard (3DES), minimum 168-bit key, encrypted algorithms.

Please refer to "KRA SOP QA-001 Participant File Standards" and "KRA SOP QA-003 Case Note Standards" for PII and PHI requirements related specifically to participant files and case notes.

* * *