Acceptable Practices Terms and Agreement for the FY 2013 HUDQC Study

Purpose

The purpose of this document is to communicate the acceptable behavior of ICF International (ICF) employees assigned to the HUD Quality Control for Rental Assistance Determinations Study (ICF Macro Contract # GS-23F-9777H; Task Order # CHI-T0001, CHI-01102), to ensure the integrity and protection of the information assets, and to obtain by written signature, agreement to the terms described.

Scope

This policy applies to all ICF employees assigned to the HUD Quality Control for Rental Assistance Determinations Study (HUDQC), and applies to information in electronic form, paper form and any verbal information received or given out during the course of the study.

Study Goals

The goal of the HUDQC study is to determine the amount of dollar error associated with determining eligibility for assisted housing and calculating the household's portion of the rent. In order to achieve the study goals, an extensive amount of information, from both tenants and projects selected for the study, is collected electronically and via paper documents by employees across the country and in Puerto Rico.

Objectivity Regarding Data Collected

In support of the goals of the study, any employee charged with collecting, seeking clarification of, reviewing, analyzing or in any way working with the data related to the HUDQC study, must do so objectively and without regard to how it might affect the outcome of the study. Employees will collect complete and accurate data and will be objective in all dealings with study participants. Employees will voice no opinions they may have about assisted housing, assisted housing tenants, and how assisted housing programs are administered and will not discuss their opinions with study participants (including households included in the study, PHA/project staff and HUD personnel).

Use of Equipment

Physical Security and User Access for the Laptop Computer. Only individuals employed by ICF to work on the HUDQC study shall have access to their issued laptop computer. Access by all other individuals is strictly prohibited. Users must physically lock their issued laptop computer with the supplied laptop security cable when feasible, and always when the laptop computer will be unattended. Users must keep their issued laptop computer in their possession at all times. The laptop computers are not to be checked in airlines luggage or with hotel porters. Users will contact their field supervisor or other appropriate HUDQC/ICF personnel immediately if they observe or suspect that the laptop computer has been tampered with in any way.

Users must not change their password(s). Users must keep their password(s) secret and never disclose it to anyone, including other HUDQC staff. Users must never write down or otherwise

record a readable password and store it near the laptop computer to which it pertains. Users must lock their laptop computer with a password when the laptop computer will be unattended. If a user realizes that someone may have obtained their password(s), they must contact their field supervisor or other appropriate HUDQC/ICF personnel immediately for guidance.

Unacceptable Use of the Laptop Computer. Users must not delete, disable, deactivate, or uninstall any software or services installed prior to the issuance of the laptop computer. Users must not install any third party software. Users must not download or install pirated or other illegal software or material. Users are prohibited from connecting any external device to the laptop computer. This includes, but is not limited to, USB external drives and mobile phones. The exceptions for external devices that may be connected to the laptop computer are the supplied peripheral devices such as the external mouse and mobile broadband modem, and a 'plug-and-play' printer as long as it does not require third party software to function properly.

Definition of Terms

Personally Identifiable Information. Personally Identifiable Information (PII) refers to information that can be used to uniquely identify, contact, or locate a single person or can be used with other sources to uniquely identify a single individual. PII includes, but is not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity such as a name, social security number, date and place of birth, mother's maiden name, or biometric records. PII is sensitive information and should be safeguarded at all times.

Data Confidentiality Policy

General. The HUDQC study collects a large amount of sensitive information that contains PII. The employees working on the study will have access to sensitive information that is protected under Privacy Act (5 U.S.C. 522a), which must not be disclosed to unauthorized persons. Any government information made available to employees, as a member of the project team, shall be used only for the purpose of carrying out the requirements of the project and shall not be divulged, or made known, in any manner, to any person who is not a member of the project team, without written authorization from the project director. Any person who discloses confidential information, by any means, for a purpose or to any extent unauthorized by the study terms contained herein, may be subject to criminal sanctions as imposed by 18 U.S.C. 641.

All information obtained, from formal interviews, in casual conversations or observations, or from hardcopy documents, will be treated as confidential and must not be disclosed to any parties not authorized to have access to such information, including, but not limited to, other households included in the study, PHA/project staff, and HUD personnel.

Tenant files may not be removed from project offices by HUDQC field interviewers. Data abstraction must occur at the project office. All paper documents that contain any PII will be stored so that they are not accessible to non-study staff and will be sent to ICF study headquarters as instructed. No copies of documents with PII will be retained by employees after data collection is complete.

The electronic hardware and software issued to employees has been set up with specific safeguards and restrictions implemented for the security of the information. It is the responsibility of employees to use the hardware and software only as they were intended and as they were trained to do.

It is also the responsibility of employees to understand the sensitive nature of the data being collected, and to ensure the proper methods of storage and transmission of the data as outlined in this document.

Electronic Data Storage & Transmission. Users will only enter and keep electronic data on the issued laptop computer. Users are prohibited from storing electronic data on any computer or electronic device not issued to them by ICF /HUDQC staff, including, but not limited to, USB external drives and mobile phones.

Users must only transmit electronic data containing PII by the *Field Data Transfer* program pre-installed on the issued laptop computer or by the study's secure website (https://hudqc.icfwebservices.com). Users must never request to receive sensitive information or PII from a third party via email. Users should direct the third party to the study's secure website (https://hudqc.icfwebservices.com) when requesting the information.

Email. Users must use only their provided email addresses authorized to perform work for ICF /HUDQC. Users are prohibited from auto-forwarding messages directed to their provided email address to an external email address. The provided email addresses are not encrypted or secure. Thus, users should never transmit PII by email. This includes the subject line or body of an email, and in any accompanying attachment. The anonymous identifier assigned to each household (i.e., C/P/C) should be used instead of PII in any email subject or body. Any potential attachment that would include PII should only be sent to study headquarters via the study's secure website (https://hudqc.icfwebservices.com).

Internet. Users must use the Internet on their issued laptop computer only for business purposes. Users are prohibited from using all types of peer-to-peer file-sharing software or services (e.g. Bit Torrent) on their issued laptop computer. Users must not allow access to their issued laptop computer through the Internet unless authorized by ICF /HUDQC office staff.

Users must only connect their issued laptop computer to the Internet by the service provider and mobile broadband modem provided with the laptop computer. Users should never connect their laptop computer to any other network. This includes, but is not limited to, a public wifi hotspot or a private home network. If a user is unable to connect to the Internet by the service provider and mobile broadband modem provided with their laptop computer, the user should contact his/her field supervisor or other appropriate HUDQC/ICF personnel for guidance. HUDQC staff reserve the right to monitor how the laptop is accessing the Internet or other networks.

Paper Document Data Storage and Transfer to Headquarters. Paper documents that contain PII will be handled and transferred to headquarters with the utmost regard for the privacy of the participants in the study. All pre-printed, photocopied, and handwritten notes will be stored in

the folders provided. The folders and documents will be stored and transported using a closed container; preventing unauthorized persons from viewing any PII (including name and telephone numbers of study participants).

When authorized by study protocol, paper documents may be faxed to the secure fax machine at study headquarters only through the hands of the employee. Authorized faxing may originate from a fax machine located in the project participating in the study, or from a private fax machine located in the employee's home. Documents may not be faxed from public fax machines when a store employee, hotel employee, or other unauthorized person must handle the documents. If an employee is receiving a fax from headquarters, it must be received into the hands of the employee. Faxed pages originating from headquarters to the employee may not be left unattended at any fax machine where unauthorized persons could possibly have access to the documents.

All paper documents sent to headquarters should be transferred by the employee using the FedEx envelopes and pre-printed air-bills provided. The envelope should be securely sealed and transported to the FedEx drop box or FedEx store with appropriate precautions taken to assure the security of the package and the enclosed documents. FedEx envelopes containing study materials should not be given to a third party, (e.g., family members, hotel personnel, friends) for any reason including delivery to a FedEx drop box or store.

Reporting of Disclosures

Employees shall promptly and immediately report to their supervisor any knowledge of uses, transmissions, losses, or other disclosures of paper or electronic information, whether intentional or unintentional, that are not in accordance with this document or applicable law. If their supervisor is not available, an alternate supervisor, the data collection manager, data quality manager, systems manager, project director, or deputy project director at ICF should be contacted. In addition, and to the maximum extent practical, users shall assist in mitigating any harmful effect of any unauthorized use or disclosure of such information.

My signature below signifies my understanding of the *Acceptable Practices Terms and Agreement for the FY 2013 HUDQC Study* document and my agreement to adhere to the policies as described**.**

Print Name: _____

Signature: _____

Date: _____