Protecting FTI in ACA Printed Notices
Rev. 01/2016

Marketplaces planning to send Advance Premium Tax Credit (APTC) termination notices based on receipt of FTI must take care to protect the confidentiality of the data. All information received by the Marketplace from the IRS for purposes of verifying income or making an eligibility determination for insurance affordability programs is protected tax return information of the individual taxpayer to whom it pertains (by SSN). APTC termination notices must be addressed to the primary tax filer and mailed (i.e. same as Form 1095-A Marketplace Insurance Statement) to prevent improper disclosure to other individuals or third parties. Such notices contain protected FTI and must be printed and mailed and may not be uploaded to online electronic accounts to prevent access or viewing by anyone other than the subject taxpayer. Notices that contain FTI require continuous safeguard protection. Whenever FTI is printed, additional physical security protections along with record keeping logs to track the chain of custody, and secure handling and storage of FTI in paper form, must be employed at all times to prevent unauthorized disclosure or inadvertent access by unauthorized individuals.

Federal Tax Information (FTI): FTI is any return or return information received from the IRS or any secondary source which is protected by the confidentiality provisions of Internal Revenue Code section 6103. FTI includes any information created by the Marketplace that is derived from return or return information. For example, if a list of individuals is generated based off the Failure to Reconcile (FTR) Response Code, then the list itself is considered FTI of those individuals and must be also be properly safeguarded.

Vendor support: If a vendor has access, or vendor equipment is used for the printing of the notices containing FTI, and the Marketplace has not previously notified the IRS (i.e. the vendor is not already listed on the agency's annual Safeguard Security Report SSR), the agency must notify the IRS using the 45-Day Notification process outlined in Publication 1075 section 7.4 *45-Day Notification Reporting Requirements*. Any agency contracts with a vendor involved in processing FTI in paper form must also include Publication 1075 Exhibit 7 language to ensure contract personnel maintain the confidentiality of FTI. This may include contracts with a print facility, printer, mail courier, or any other vendor involved in the printing process. Vendor personnel are responsible for the continuous protection of FTI, including tracking the location of FTI from receipt through final disposition. Contract employees handling FTI require awareness training and signed confidentiality statements prior to initial access to FTI and annually thereafter. The agency is responsible for oversight of its contractors in possession of FTI; including ensuring IT systems comply with IRS Publication 1075. Routine internal inspections of contractor facilities and FTI handling procedures in accordance with Publication 1075 must be conducted every 18 months at a minimum.

Safeguard Security Report SSR: The agency must update the annual SSR with the description of any new path of FTI and provide an updated data flow outlining the updated flow from creation of the FTI through mailing to the client and outline processes for notices returned either by the client or the USPS.

Electronic Transmission: All electronic transmissions of FTI needed to prepare the notice must be encrypted using FIPS 140-2 validated cryptographic modules. NIST SP 800-53 controls are the baseline used to establish safeguards security protocols. Agencies are encouraged to review supplemental guidance provided within NIST SP 800-53.

Electronic Storage: Copies of retained notices and any indicator that such notice containing FTI was sent is also considered FTI and must be restricted from access by unauthorized personnel. Any system that contains either a copy of the notice or an indicator this notice was

sent must be outlined in the agency's SSR and employees with access need safeguard training and signed certifications. These systems and employees with access are subject to all Publication 1075 requirements.

Printing: Printing must be accomplished in a secure area to ensure control of all printed output. The agency must control physical access to information system output devices to prevent unauthorized individuals from obtaining the output. While the notices are being processed, access must be restricted to only authorized individuals.

Mail containing FTI must be securely stored and safeguarded until transferred to the custody of the U.S. Postal Service (USPS). Even when enveloped and metered (or stamped), the mail should be kept in a secure location and locked in secure containers overnight if not mailed until the next day.

When using a multi-functional printer-copier device for printing, additional controls must be employed to protect FTI converted from electronic to paper form. These controls are outlined in Publication 1075 section 9.4.9 Multi-Functional Printer-Copier Devices.

Handling and Shipping: When FTI is transported from one location to another within the agency or between the agency and a vendor, care must be taken to ensure that notices are not misplaced or available to unauthorized personnel. Only those employees who have a need-to-know and to whom disclosure may be made under the provisions of the statute should be permitted access to FTI. In the event the material is hand carried by an individual in connection with a trip or in the course of daily activities, it must be kept with that individual and protected from unauthorized disclosures. For example, when not in use the material is to be placed in a locked security container (e.g., turtle case, cabinet, or drawer). All shipments of FTI (including electronic media) must be documented on a transmittal form and monitored to ensure that each shipment is properly and timely received and acknowledged. All FTI transported inter-agency through a mail or courier/messenger service must be double sealed; that is one envelope within another envelope. The inner envelope should be marked confidential with some indication that only the designated official or delegate is authorized to open it. The external packaging should not be marked and may in fact, put the information at additional risk by identifying sensitive contents. Using sealed boxes serves the same purpose as double sealing and prevents anyone from viewing the contents thereof. Lost or damaged packages require incident reporting in the event FTI is lost or available to unauthorized recipients.

Important: When mailing correspondence directly to the subject taxpayer, double wrapping and labelling of the correspondence is not required. Use a single envelope but ensure that sensitive information is not viewable (i.e. SSN or any FTI). Do not identify the envelope as containing FTI. Undeliverable mail returned to the agency, must be treated as FTI. It may be destroyed and recorded, or if opened and handled, safeguard record keeping requirements apply.

Paper Storage: Paper copies of paper notices retained in agency records must be properly labeled so they are identified as FTI, including the outside of case files in which they are retained. The notices and files must be securely stored in locked secure storage with two barriers of protection, preventing access to only authorized individuals until destruction. Electronic copies of the notices must not be kept and loaded into an agency application where clients could have access to view these documents as this could be an unauthorized access of FTI.

Destruction: Notices containing FTI that are returned undeliverable, (e.g. due to address errors) must be continuously safeguarded if retained in agency records. For this reason, returned mail should be treated as an incoming source of FTI, and therefore logged per Publication 1075, section 3.2, secured, and destroyed appropriately. Any paper material generated from FTI; such as extra copies, photo impressions, computer printouts, reports, lists or notes or work papers must be destroyed by burning, mulching, pulping, shredding, or disintegrating.

Policy: The agency must establish a written policy which is communicated to all employees that mitigates the possibility of distribution via email or electronic faxing, and the appropriate protections for the information. Publication 1075 requires each agency disseminate a policy pertaining to the emailing and faxing of FTI, even if prohibited.

IRS Publication 1075 References:

3.2 Electronic and Non-Electronic FTI Logs;
3.3 Converted Media;
4.3 Restricted Area Access;
4.4 FTI in Transit;
5.4 Controls over Processing;
6.4 Internal Inspections,
7.4 45-Day Notification Reporting Requirements;
8.3 Destruction Methods;
9.4.3, Email Communications;
9.4.4, Fax Equipment;
9.4.9 Multi-Functional Printer-Copier Devices; and
Exhibit 7, Safeguarding Contract Language for General Services