Safeguards Technical Assistance Memorandum for Contractor Data Migration of Federal Tax Information (FTI) into State Integrated Eligibility Systems (IES)

Access to certain FTI by contractors or by multiple agencies within the same application is generally prohibited. However, with proper approval from the IRS Office of Safeguards, access of FTI utilizing an IES may be granted in situations evaluated by IRS. The following guidelines must be followed.

The IRS Office of Safeguards has recently observed an increase in the number of agencies requesting information on IRS approval when migrating to Integrated Eligibility Systems (IES) to process client accounts including federal tax information (FTI). These new systems present opportunities for agencies to provide a convenience to clients as well as replace legacy agency systems with considerable financial assistance from the federal government. The migration and protection of FTI in this new system creates new risks to FTI and properly restricting access to FTI housed in these new systems.

An IES utilizes an efficient single point of entry that will allow seamless eligibility processing for applicants requesting assistance. The system generally supports eligibility for Medicaid and Children's Health Insurance Program (CHIP), Temporary Assistance for Needy Families (TANF), the Supplemental Nutrition Assistance Program (SNAP) and other state-administered assistance programs, such as Women, Infants and Children (WIC), Child Care and the Low Income Home Energy Assistance Program (LIHEAP) as well as Child Support Services. FTI is obtained under various Internal Revenue Code (IRC) § 6103 disclosure authorities but may not be shared across programs nor accessed by state agency employees for unauthorized program uses.

State information technology (IT) officials are generally engaging contractors to design, develop, and implement these integrated systems. State agencies authorized to receive FTI from the IRS Disclosure of Information to Federal, State, and Local Agencies (DIFSLA) and SSA Beneficiary Earnings Exchange Record (BEER) to administer TANF, SNAP and Medicaid programs under the authority of IRC § 6103(l)(7) are prohibited to contract for services that allow disclosure or access to the FTI. State Child Support Enforcement Agencies (CSEA) authorized to use FTI under IRC § 6103 (l)(6),(l)(8), and (l)(10) may only permit contractor access for purposes of collection and disbursement of child support payments with limited access to FTI - only the address, SSN, and the amount of the refund offset, for the purposes of establishing and collecting child support obligations as provided by IRC § 6103(l)(6)(B). Agency contractors with access to FTI received under IRC § 6103(l)(6),(l)(7),(l)(8), or (l)(10) must have an encryption barrier in place during migration.

IES may contain FTI received under various code authorities from multiple agencies within the one system. IES could contain information provided to Medicaid/ACA agencies under IRC § 6103(l)(21), SNAP, TANF, Medicaid under IRC § 6103(l)(7), Child Support Agencies FTI provided under IRC § 6103 (l)(6),(l)(8), and (l)(10). The IRC does not permit the sharing or access of FTI between state agencies. FTI can only be used for the purpose it was provided to the agency under the code authority it was provided. Additionally, information must be segregated so only the authorized individuals have access to the FTI obtained from their perspective code authority.

Whether currently in use or planned to be deployed, FTI safeguarding measures required by the IRS Office of Safeguards must be in place given the security vulnerabilities associated with Integrated Eligibility Systems. This memo provides the policy requirements for ensuing the confidentiality of FTI is maintained by agencies that utilize IES.

Requirements for Contractor access to restricted FTI in an Integrated Eligibility System

To utilize an IES that contains FTI, the agency must meet the following requirements:

1. 45 Day Notification process outlined in Publication 1075 must be followed.
2. If a contractor is being utilized with access to FTI special procedures must be followed.
3. All FTI must be encrypted in transit end to end.
4. FTI segregated by IRC 6103 code authority
5. Agency Oversight

These requirements are explained in detail in the sections below.

1. 45-Day Notification Reporting Requirements

IRC § 6103 limits the usage of FTI to only those purposes explicitly defined. Due to the security implications, higher risk of unauthorized disclosure and potential for unauthorized use of FTI based on specific activities conducted, the Office of Safeguards requires advanced notification (45 days) prior to implementing certain operations or technology capabilities that require additional uses of the FTI.

All agencies intending to re-disclose FTI to contractors must notify the IRS at least 45 days prior to the planned re-disclosure. Contractors consist of but are not limited to:

- cloud computing providers
- consolidated data centers
- off-site storage facilities
- shred companies
- IT support
- tax modeling/revenue forecasting providers.

The contractor notification requirement also applies in the circumstance where the contractor hires additional subcontractor services. Approval is required if the (prime) contractor hires additional subcontractor services in accordance with Exhibit 6, *Contractor 45-Day Notification Procedures*.

If the IES system will also be comprised of a data warehouse, the agency must provide written notification to the Office of Safeguards, identifying the security controls, including FTI identification and auditing, within the data warehouse. For additional data warehouse guidance, see Exhibit 10, *Data Warehouse Security Requirements*.

2. Contractor FTI access

Agencies must ensure that contractor access to systems that receive, process, store, or transmit FTI is restricted. This distinction should be made at an agency level after determination of whether contractors can access FTI. Contractor access to systems for the purposes of development and deployment must also be restricted where FTI is determined to be in use. In this event, specific timeframes for contractor access must be listed on the 45-Day Notification which will be agreed upon by the agency and the Office of Safeguards. The agency must implement encryption as a barrier to contractors and the agency must retain the encryption keys. The only FTI access administrators would have with these methods in place is delete only access. Contractors with access to FTI must receive FTI awareness training and all contracts with the agency must contain the Exhibit 7 Safeguarding Contract Language. This written agreement for services must be documented and included with the 45 Day Notification request.

3. FTI Encrypted in Transit

All electronic transmissions of FTI must be encrypted using FIPS 140-2 validated cryptographic modules. A product does not meet the FIPS 140-2 requirements by simply implementing an approved security function. Only modules tested and validated to FIPS 140-2 meet the applicability requirements for

cryptographic modules to protect sensitive information. NIST maintains a list of validated cryptographic modules on its website http://csrc.nist.gov/.

4. FTI Segregated by IRC 6103 Code Authority

The FTI must be physically/logically segregated by code authority (i.e. data set) and access restricted by system processes and applications for authorized program uses. Agency personnel can only have access to FTI provided under the code authority to their agency. FTI is not permitted to be shared among agencies nor re-disclosed to other agencies. Steps must be taken to ensure FTI contained within an IES are segregated by agency for both backend database and frontend application access. Access should be authorized for information systems that receive, process, store, or transmit FTI based on a valid access authorization, need-to-know permission, and under the authority of the provisions of IRC § 6103.

5. Agency Oversight

An authorized state employee must be present onsite and oversee the vendor providing the service during the process. The work must be performed at an approved state facility, not at a vendor site and all appropriate safeguard controls must be employed (i.e. production level system controls, training certifications, data segregation, labelling, etc.)

Resources

Additional information can be found in the following documents:

- IRS Publication 1075
- Additional Requirements for Publication 1075
- Recommended Security Controls for Federal Information Systems and Organizations, Revision 3" title="NIST SP 800-53, *Recommended Security Controls for Federal Information Systems and Organizations,* Revision 3">NIST SP 800-53, *Recommended Security Controls for Federal Information Systems and Organizations,* Revision 3
- Guide to General Server Security" title="NIST SP 800-123, *Guide to General Server Security*">NIST SP 800-123, *Guide to General Server Security*

References/Related Topics

- Publication 1075, Tax Information Security Guidelines for Federal, State and Local Agencies and Entities
- Safeguards Program
- Additional Requirements for Publication 1075