



Adhering to IRS Publication 1075 Guidelines

Presented by:
Chuck Adelman, Tax & Revenue Practice Leader

AUGUST 2009



Tax Implementation Experience

- Full-time:
New Jersey, Kansas, New York City, **Connecticut**,
Ireland, **Maryland, North Carolina**, Ohio, Detroit, Los
Angeles
- Part-time:
Maine, Pennsylvania, California, Tennessee, Puerto Rico,
Washington D.C., **Arizona**, Singapore, Malaysia,
Australia, **Kentucky**

2 / AUGUST 2009



Presentation Ground Rules

- I am not a representative of the IRS.
- The views expressed by Chuck Adelman are not necessarily those that would be expressed by each and every IRS representative.
- IRS Publication 1075 cannot cover every possible scenario required to help agencies protect taxpayer data.
- IRS Publication 1075 continues to evolve:
 - Issued in June 2000
 - Updated in February 2007
 - Updated (again!) in December 2007
 - December 2007 is still the latest (for now)

Why 1075?

- Originally, social security numbers were used solely by (surprise!) the Social Security Administration when this agency was formed during the New Deal.
- Over time, the SSN has been used as the "de facto" identification number for virtually all U.S. residents.
- Potentially severe implications if taxpayer data (in particular SSNs) are not adequately protected – taxpayers need a high degree of confidence.

Moving From Paper to Electronic Media

- When the IRS first began sharing information with state agencies, all information was paper based.
- Although more information is being sent electronically (and less via paper), several provisions still have a "paper paradigm".
- Maintaining 1075 compliance is easier in an "electronic paradigm" than with a "paper paradigm".

1075 Compliance Focuses on 6 Areas:

- Record keeping
- Secure storage
- Restricting access
- Other safeguards
- Reporting requirements
- Disposal

Record Keeping

- To better adhere to record keeping provisions, it is recommended that only electronic files (not paper files) be obtained by the IRS.
- Electronic files can be handled only by an authorized employee(s), who must log information such as date received, control number, recipient, number of records, movement, and disposal date.
- It is recommended that there be one authorized individual, and one backup.

Secure Storage

- It is recommended that Federal data be kept in a locked metal container (that can resist forced penetration) in a locked room (solid walls) with different keys.
- Door hinge should be on the inside!
- Limited number of authorized individuals should have key access (e.g., one assigned, one backup per each).
- Vent size should not allow human access.
- Minimize/eliminate the need for custodial and/or maintenance requirements.

Secure Storage (continued)

- To minimize handling/transportation of FTI, it is recommended that information from magnetic tapes, etc. be uploaded into a secure database (completely separate from other agency databases), where only authorized individuals will have access.
- Commingling is allowed only with data warehouses, and only if proper security controls are installed (monitoring software down to the individual field level, etc.).
- Data warehouse vendors should certify that their software is 1075-compliant.
- There should be highly-restricted data access.

Restricting Access

- All information strictly on a "need to know" basis.
- It is recommended that automated programs (i.e., not "eyeballing") be used for identifying potential cases.
- Keeping all information electronic, minimizes "manual browsing."
- Federal information should be accessed only for the handling of a specific "case", and the record of accessing Federal information should be captured in the case history.

Other Safeguards

- Employee awareness
 - Formal training
 - Security articles in newsletters
 - Warning banners
 - Forwarding articles
 - More training
- Internal inspections – don't wait for the IRS
- Never turn over data security responsibilities to a non-government employee/entity

Other Safeguards (continued)

Security Awareness Questions:

- Have written instructions been issued to employees/contractors concerning the handling, controlling and securing of FTI?
- Have employees/contractors received formal or informal training?
- Are employees aware of the disclosure and penalty provisions of the law?
- Are employees aware of emergency procedures, particularly those regarding the securing of tax information?
- Are employees advised annually of the provisions of IRC § 7213, IRC § 7213A and IRC § 7431?
- Have the requirements for unauthorized access (UNAX) detection and training been met per the Taxpayer Browsing Protection Act?
- Are the initial certification and annual recertification documented and placed in agency and/or contractor files?

Reporting Requirements

- Safeguard Procedures Report (SPR)
 - Responsible officers
 - Data location
 - Flow of data (recommendation: keep it electronic!)
 - System of records (again, easier if it is all electronic)
 - Secure storage
 - Restricting access
 - Disposal
 - Security
 - Awareness programs

Disposal

- Return information to the IRS, and receive confirmation
- Destruct information – again, it is much easier if it is all electronic (i.e., no shredding, no pulping, etc.)

Design Guidelines

- Upload FTI into separate data base tables (with extremely restricted access); do not add FTI into existing data base tables
- Create separate screens/windows for viewing FTI (again with extremely restricted access) with appropriate warning banners; do not add FTI elements to existing screens/windows
- Do not create any reports that will have FTI
- Phrase correspondence to minimize (or eliminate) FTI; avoid making references to IRS (if possible)

General Guidelines

- Get the IRS involved early
- IRS seems to be most interested in where FTI will reside, and how the information will "flow" throughout the organization
- Keep control over taxpayer data; do not outsource to a third party
- IRS data is for matching against state/local revenue data only; it should not be used for validating non-revenue data
- Get the IRS involved early (yes, I know that I stated this before)
- Ask other states if they have 1075 plans that have been reviewed by the IRS

Contact Information

Chuck Adelman
EDS, an HP company
Tax & Revenue Practice Leader
State & Local Division

Chuck.Adelman@eds.com
(908) 397-2112



EDS and the EDS logo are registered trademarks of Hewlett-Packard Development Company, LP. HP is an equal opportunity employer and values the diversity of its people. ©2009 Hewlett-Packard Development Company, LP.

Behind success there's

