Maintaining Compliance with Two Critical Privacy Safeguards

RevSpring

Understanding Pub 1075 & Pub 4812

RevSpring spoke with industry regulatory expert Rob Horwitz, Esq. from Horwitz Law Firm, PLLC to understand more about these Publications, and what ARM firms should be doing to comply.

Account receivables management (ARM) organizations are familiar with a long—and growing—list of compliance and privacy obligations. Over the past decade, the pace of new mandates has multiplied as federal and state regulators seek to introduce or update protections for consumers, address the use of new technologies and a wider range of communications channels, and ensure data privacy.

But two important regulations surrounding personal information have been in place for years. IRS Publication 1075 (Pub 1075), "Tax Information Security Guidelines for Federal, State and Local Agencies and Entities" was implemented in 2000. IRS Publication 4812 (Pub 4812), "Contractor Security and Privacy Controls", was enacted in 2013.

While these publications are clearly not new, adherence to their requirements requires ARM firms of all types—including those who are subcontracted to help with collection—to maintain certain stringent data and processing standards. ARM firms that aren't following their requirements may be at risk for financial penalties or even criminal charges.

Q: Why did the IRS release these Publications?

To foster a tax system based on voluntary compliance, it is critical that the public has a high degree of confidence that personal and financial information maintained by the IRS is protected. The IRS has long required companies that receive Federal Tax Information (FTI) in any capacity to have safeguards in place to prevent an unauthorized disclosure of that FTI.

FTI protections date as far back as 1976, when Internal Revenue Code Section 6103 was established. Code 6103 stipulates that the IRS must protect all the personal and financial information furnished to the agency against unauthorized use, inspection or disclosure.

Q: Who is required to follow the FTI safeguards?

The mandates for FTI cover any tax return or tax return information received from the IRS or secondary source (e.g. Social Security Association). Other Federal, State and local authorities that receive FTI directly from either the IRS or from secondary sources must also have adequate security controls in place to protect the data they receive. Which—in a nutshell—means ARM organizations that handle tax information are required to comply.

Q: What Is Publication 1075?

Pub 1075 is a set of guidelines for all organizations possessing FTI. It features information on the controls, safeguards, practices, and policies that organizations—including their contractors and recipient agencies—must follow to safeguard against the improper disclosure of FTI data. It includes operational, managerial, and technical security controls.

To be considered compliant with Pub 1075, organizations have to show the IRS that they are following the guidelines, and capable of actively protecting the confidentiality of FTI information through established safeguards.

If the data is stored digitally, then restricted access protocols will need to be followed to ensure that the network and subsequent data remains secure.

Q: What Is Publication 4812?

The intent of Pub 4812 is to establish privacy and security requirements specific to the IRS contracting environment. It identifies security controls and privacy requirements for contractors (and their subcontractors) that handle or manage IRS Sensitive But Unclassified (SBU) information on or from their own information systems or resources.

Q: How can an organization remain compliant with Pubs 1075 and 4812?

If an organization is to remain compliant with Pubs 1075 and 4812, then all FTI data it receives and handles has to be secure. To do this, an organization needs to implement certain processes, checks, measures, and safeguards to ensure that the FTI data remains confidential and safe. These include written controls and annual reporting of any violations of the controls and safeguards including the security of IT systems and monitoring who has physical access to systems and processing environments. Contingency plans and the incident response system should also be assessed annually.

Q: Do the rules vary depending on the format of the data?

No. The rules apply regardless of the storage method used (i.e. paper or electronic). The guidance is designed to cover every state of the FTI data, from receipt to transfer, storage to usage, access to transmission, and finally its disposal. The data needs to remain safe, secure, and confidential at all stages.

Q: How should data be stored? Is it permissible to dispose of or delete data?

There are specific details regarding the physical and electronic security of FTI data. Guidance is provided regarding locks, vaults, safes, keys, authorized access, and secure transportation of the data. To remain compliant with this control, firms need to review the security of their organization's devices, media storage solution, and network.

If the data is stored digitally, then restricted access protocols will need to be followed to ensure that the network and subsequent data remains secure. Whether it is in physical or electronic form, FTI data has to be disposed of securely and properly in accordance with established IRS guidelines.

Q: What are some of the requirements around using data? Do we need to limit who has access to information and how they access the information?

FTI data, whether electronic or paper, should be accessible only to authorized parties. A secure and accurate record keeping system should be established. This record keeping system should include all the FTI records, any documents or data associated with the FTI records, and information regarding access rights to the data. As part of secure storage controls, a log should be kept regarding the access, transfer, usage, storage, and eventual disposal of the FTI records.

Q: Is training required for people who handle FTI?

Yes. All employees who are responsible for handling, storing, securing, transporting, or the disposal of FTI data must receive the appropriate security training. Additionally, employees will need to receive an annual certification. Annual inspections are required to ensure that the proper methods are implemented throughout the lifetime of FTI data. Firms that handle or process FTI on a subcontract basis aren't usually audited directly by the IRS, but such firms should provide reports and certifications to their contracting firms who, in turn, usually report this data to the IRS. As part of the audit of the subcontractor's client, the IRS may inspect the subcontractor's FTI processing facility.

Q: The ARM industry shares information through electronic files and transfers. Are there requirements for computer system security?

Yes, and this safeguard is quite complex. It includes cybersecurity best practices, such as File Integrity Monitoring and Security Configuration Management.

Q: What happens if FTI data needs to be transcribed or used in a different format? For example, can firms extract FTI from data files to create collections notices?

Pub 4812 provides very specific guidance on necessary physical access controls if the FTI is reduced to written form. For example, if the FTI is being transformed from data to paper to create a collection notice to a delinquent tax paper, the production floor must be designated a secured, limited access area. This area can be accessed only by FTI authorized/certified personnel. In other words, FTI and non-FTI work should not be processed/produced in the same production area unless all personnel with access to that area are FTI certified.

There are additional physical and space controls. In order to process FTI and non-FTI work within the same facility, a company needs a secure room/space for the FTI work that is enclosed by slab-to-slab walls or other compensatory measures and otherwise meet the requirements of the Publication, including the guidance in Addendum D.

All employees who are responsible for handling, storing, securing, transporting, or the disposal of FTI data **must receive the appropriate security training.**

Failure to secure information and/or accidentally mishandling, storing, using, transmitting, or disposing of FTI could result in lawsuits, loss of business/contracts, significant fines and criminal charges.

Q: What happens if there is a breach or if a firm accidentally misuses FTI data?

The growing list of regulations to safeguard consumer information has made the consequences of a breach more serious than ever. In addition to reputational risk, failure to secure information and/or accidentally mishandling, storing, using, transmitting, or disposing of FTI could result in lawsuits, loss of business/contracts, significant fines and criminal charges. Annual testing and certification and ongoing maintenance of protocols can pose a significant burden—and risk—for some firms. I recommend assessing whether a subcontracted firm has the scope and resources to manage the requirements of Pub 1075 and Pub 4812 on an ongoing basis.

RevSpring has a thorough series of procedures in place for handling FTI data. With specific, segregated processing environments, robust employee training, and controls around data security and storage, we are focused on delivering effective, compliant support for ARM firms of all types.

Rob Horwitz of Horwitz Law Firm, PLLC (www.horwitzfirm.com) is a litigation and compliance lawyer with over 25 years of experience representing ARM companies as retained and internal counsel. Since 2007, Rob has specialized in defending companies in class actions and individual cases filed under the FDCPA, FCRA and TCPA, in addition to providing advice on all aspects of those federal statutes.

Disclaimer: The contents of this resource are not intended to serve as legal or any other advice.

RevSpring leads the market in financial communications and payment solutions that inspire action—from the front office, to the back office, to the collections office. North America's leading healthcare organizations, revenue cycle management and accounts receivables management companies trust RevSpring to maximize their financial results through dynamic and personalized print, online, phone, email and text communications and payment options. Using proprietary data analytics to tailor the engagement workflows to fit individual circumstances and preferences, RevSpring solutions improve the consumer financial experience and drive better outcomes.

To learn more about RevSpring's expertise and focus in Accounts Receivable Management, visit www.revspringinc.com/financial-services, email info@revspringinc.com or call 248.567.7300.

RevSpring

