

## Confidentiality and Security of Taxpayer Data

Protecting the confidentiality and security of taxpayer data has always been a priority focus for this program and its volunteers. In sharing their sensitive personal data with us, taxpayers have put their trust in us and given us a major responsibility to protect that information. In today's age of identity theft, this focus is even more critical and urgent. Leaders *must* ensure that all volunteers understand these confidentiality and security responsibilities and abide by them.

There are many steps we can take to help ensure that we honor that trust and protect taxpayer information. This section is intended to provide you with AARP Tax-Aide required and recommended security controls that will help preserve the confidentiality and privacy of taxpayer data.

### Data Security

1. *All* volunteers must sign the Standards of Conduct statement (IRS Form 13615), which is provided in the IRS test or as a separate form. That statement has three bullets addressing the protection of taxpayer data:
  - ❖ I will safeguard the confidentiality of taxpayer information.
  - ❖ I will exercise reasonable care in the use and protection of equipment and supplies.
  - ❖ I will not solicit business from taxpayers I assist or use the knowledge I have gained about them for any direct or indirect benefit for me or any other specific individual.

Certification of Counselors has three significant and critical components. First, Counselors *must* train and pass the IRS test. Second, all must agree to the Standards of Conduct and note that agreement by signing the statement. Third, all must attend formal policy and administrative training annually. These are significant commitments that every Counselor must take seriously.

2. Information provided for tax return preparation *must not* be shared with anyone who does not have a need to know. Individuals have the need to know if their involvement is required to accurately process the information to its final disposition. Examples of "need to know" would include, sharing information for the purpose of obtaining guidance in tax return completion, for electronic transmission, and/or for quality review of the finished tax return. In accordance with 18 USC 1905, which applies to Tax Counseling for the Elderly grantees including AARP, it is not acceptable to share information with others, even with other volunteers, if their involvement in the tax return preparation is not required. For instance, sharing income information, birth dates, or even the marital status of taxpayers with other volunteers, taxpayers, family, or friends as a matter of curiosity or interest is not acceptable. However, per Internal Revenue Code 7216, aggregate or summary taxpayer data can be shared, but only if that data covers 25 or more returns. The data must be summary information in categories such as total EITC dollars, total Child Tax Credit dollars, etc. Of course,

the total number of returns processed is always OK to share as that number is a production count unrelated to any taxpayer data.

3. Internal Revenue Code Section 7216 provides penalties against tax return preparers who make unauthorized use or disclosure of tax return information. The IRS now requires a very specific authorization process for taxpayers to approve use and disclosure of their data to others. AARP Tax-Aide does not need to use those procedures as we do not/cannot share specific data with anyone including VITA, banks, mortgage companies, others in AARP, etc. As stated in (2) above, summary data can be shared if the data covers 25 or more returns.
4. Do **not** send taxpayer data via regular email. Taxpayer data may only be sent over the Internet by using *TaxWise* mail, or as an attachment to regular email that is in the form of a backup created by the *TaxWise* program.
5. Forms 8879, together with the taxpayer's supporting W2s and 1099 documentation, have a three-year retention requirement from the return due date or IRS received date, whichever is later. This information **must** be sent to the local IRS territory office by the end of April. Forms 8879, W2s, 1099, etc. **must not** be kept by AARP Tax-Aide volunteers beyond April 30<sup>th</sup>.

For numerous reasons, including taxpayer data security and confidentiality, all returns **must** be prepared in front of the taxpayer and all records given back to the taxpayer at the end of that assistance session. Required retention of some records for e-filing, such as W-2s and 1099s with federal tax withholding is allowed, but only until April 30<sup>th</sup> (see #6 below). Appropriate steps to secure taxpayer data must be taken at all times. All equipment on which taxpayer data resides **must** be protected by encryption software. This applies to **all** computers, removable storage devices, such as flash drives or external hard disk drives, and removable media, such as CDs and DVDs, whether this equipment is provided by AARP, the IRS, by a site or by volunteers. The only exception is for backups created by the *TaxWise* program itself. These backups are adequately protected without being further encrypted and may be stored on unencrypted storage devices and media.

Network workstation and *TaxWise Online* (TWO) computers that never have taxpayer data stored on them, or computers running *TaxWise*<sup>TM</sup> from removable data storage devices that themselves are encrypted, do not require encryption software. More information on the AARP Tax-Aide encryption software can be found on [www.aarp.org/tavolunteers](http://www.aarp.org/tavolunteers).

6. By April 30<sup>th</sup>, all taxpayer data **must** be deleted from **all** computers and removable data storage devices that have been used in the AARP Tax-Aide program, including personally-owned and loaned computers, without exception. In addition, the recycle bin in these computers must be emptied after deleting taxpayer data. For IRS-loaned

computers, use the wipe disk program loaded on them. For non-IRS equipment, use the *TPClear* program. Instructions for downloading, installing, and using *TPClear* may be found at [www.aarp.org/tavolunteers](http://www.aarp.org/tavolunteers).

7. During the season, the operating *systems* of **all** computers containing taxpayer data **must** be password-protected. Additionally, for multiple security reasons, the *TaxWise*<sup>™</sup> Admin and User accounts **must** be password-protected. If you have any questions about how to password-protect either, please see a volunteer leader at your site or go to [www.aarp.org/tavolunteers](http://www.aarp.org/tavolunteers) and see the General Security document under Security & Confidentiality for additional guidance. Passwords must not be shared with anyone who is not an AARP Tax-Aide volunteer. If you must have a written password reminder, keep it away from the computer, carrying case, or anything tax related and in a location that is not visible to others (consider putting it in your wallet or billfold, which is usually always with you and something you take care to protect). Here are some general guidelines to be followed when setting up a password:
  - ❖ Minimum length – eight (8) characters for Windows, *TaxWise*<sup>™</sup> Admin account, and *TrueCrypt*.
  - ❖ At least one letter and one number in the password.
  - ❖ Choose a password that is not a dictionary word or someone's name.
8. The AARP Tax-Aide-provided anti-virus and firewall software program must be used to protect all AARP purchased and donated computers from viruses and hackers. ***This software and license key should be used only on computers that are being used for AARP Tax-Aide business; use on any other computer is prohibited.*** Update this software at least weekly. AVG Internet Security Suite 8.5 is the current version licensed for use by AARP Tax-Aide. The license key is available in the hard copy Counselor Digest and is also contained in the document "AVG License Information" that is posted on the Technology page of [www.aarp.org/tavolunteers](http://www.aarp.org/tavolunteers).
9. If a volunteer uses a personally owned computer during the season for tax preparation, AVG or other anti-virus and firewall software must be installed (see #8 above for additional details on AVG downloads and installation). If a volunteer is not using AVG on a personally owned computer and feels that the anti-virus and firewall software currently being used is secure and reliable, regular updates **must** be performed. (At the end of the season, volunteers **must remove** all taxpayer data from their computers. Use *TPClear* (see #6 above) or delete the TrueCrypt container files having the data within them.
10. Any site that uses two or more computers should consider wired networking. In a local area networking (LAN) environment only one computer contains taxpayer data, requires *TaxWise*<sup>™</sup> updates and needs to be backed up, but all connected computers have access to all returns. Only one computer then needs to be fully secured at all times when not being used. A personal computer should not be used as a server, unless it is used **only** for the AARP Tax-Aide program during the season.
11. Wireless communication among computers continues to be evaluated but is currently

prohibited as part of the AARP Tax-Aide program. The **only** wireless configuration that may be used in the AARP Tax-Aide program is for wireless printing. To be clear, this means that the following specific uses (and others like them) of wireless communications are prohibited:

- *TaxWise* client/server networking
- Transmission of returns to CCH, either at a site or from a home computer
- Checking on such items as ESP amounts, property taxes paid bank account numbers.
- Broadband Internet access to *TaxWise* Online

These restrictions have been established with a great concern for the privacy of taxpayer data, an abundance of caution, and the need to insure full compliance with IRS directives. More networking and configuration information may be found on the Technology section of the AARP Tax-Aide Extranet, [www.aarp.org/tavolunteers](http://www.aarp.org/tavolunteers).

12. Taxpayer data must not be stored on site-sponsor-owned computers. It is advisable to use *TaxWise*<sup>TM</sup> Online when using site-sponsor-owned computers. If that is not possible as the site sponsor-owned computers do not have high speed Internet connections, run *TaxWise*<sup>TM</sup> from an encrypted removable data storage device, such as a flash drive or an external hard drive, that must be removed and taken with you at the end of each tax session. Information on how to encrypt removable data storage devices is located on [www.aarp.org/tavolunteers](http://www.aarp.org/tavolunteers) in the Technology section.
13. As of tax season 2010, authorization by the taxpayer to retain data to use for completion of the following year's tax return is no longer required. (This usage, for assisting with completion of the following year's return is not a violation of IRC Section 7216 addressed in (2) and (3) above.) For sites using TWO, all taxpayer data is automatically stored on CCH computers and no additional action is required. For sites using the desktop version on TaxWise, one person per state, determined by the SC, is allowed to retain the data. If you participate in the Data Retention program ***you must still delete the data from your computer at the end of the season. You must not retain your own copy of the data.*** It is to be backed up to a disk, flash drive, etc. AND transferred in the off season to the one person assigned the responsibility of maintaining that data in your state. The data should not be uploaded to computers any earlier than January, preferably late January. More information on Data Retention can be found in the "The Technology Management Guide" and on the AARP Tax-Aide Extranet at [www.aarp.org/tavolunteers](http://www.aarp.org/tavolunteers).
14. Securely remove all taxpayer information from hard drives before disposal of broken or surplus computers that will no longer be used in the program. Run ***TPClear*** or delete and purge all TrueCrypt container files from the hard drive. If this is not possible, remove the hard drive from the computer and take hammer to it or drill holes in the hard drive.

15. Volunteers must act in a manner that promotes confidentiality for the taxpayer. This includes how they communicate questions and issues during their sessions with taxpayers. Conversations should be held discretely; personal taxpayer information should not be left out in areas to which others may gain access, and computer screen displays should be minimized or the application closed down if a Counselor needs to leave the work area during an individual tax assistance session. If you believe that the confidentiality of taxpayer data has been compromised due to any of these types of issues:

❖ Call **1-800-424-2277, ext 36021 or ext 36027** (during business hours), or **1-202-434-6021/6027** (after hours) immediately (within 24 hours).

❖ Inform your volunteer supervisor about the situation.

### Physical Security

1. Sites **must not** be located in individual volunteers' homes, nor should volunteers prepare returns for friends or others at their or their friends' homes. Refer to the section on Site Selection for more guidance regarding sites and maintaining confidentiality.
2. Store computer equipment in a secure/locked location, if left at a site. If you take the computers home, store them inside your home in a secure and safe place.
3. Any computers on which taxpayer data is stored, and that are left at sites must be stored and secured in the area at the site that is least accessible to non-volunteers. Computer cable locks are available through the National Office for server computers that are left at sites where additional secured locked closets or cabinets are not available. If at all in doubt about the security of a server computer to be stored at a site, consider other options such as a volunteer taking it home to their residence where they know it will be secure with no inappropriate access. Computer cable locks can also be used to secure server computers during site hours, where it is physically possible to use the cable lock. Email [taxaidetech@aarpp.org](mailto:taxaidetech@aarpp.org) if you would like to request a cable lock.
4. Do not store computers in your car or leave computers unattended in a visible area of a car.
5. Before leaving your computer for a break, turning off your computer, or closing the lid on a laptop when working with taxpayer's data, you must exit *TaxWise*<sup>TM</sup> (this applies to all computers, without exception). You must also close the encryption software (on AARP Tax-Aide computers). Closing the lid on a laptop may only put the computer into a state of "standby" or "hibernation", which may mean that *TaxWise*<sup>TM</sup> is still open and the data is vulnerable.
6. Sites must be set up in a manner that minimizes the likelihood that taxpayer data can

be overheard, or seen on a computer screen or as a hard copy document, by other taxpayers.

7. Paper forms (W2s, 1099, 8879s, etc.) are very vulnerable for theft due to exposed social security numbers and other taxpayer data which is unable to be encrypted. Forms 8879 must be mailed only from locked and secure mailboxes. **All** forms and reports with taxpayer data **must** be safeguarded from being lost or stolen, particularly at sites. They should be stored in envelopes and folders out of view during site hours, and when the site is closed care should be taken to make sure they are locked away and secured.

### **Reporting a Loss**

***This covers computers, removable storage media (flash drive, floppy disk, CD) and papers lost, stolen, or damaged with taxpayer data residing on them.***

Computers, removable storage media (external drives, such as a flash drives, floppy disks, or CDs), and paper used for tax preparation, such as Forms 8879, backups and data storage, may contain information that is private to the taxpayers involved. Should these be lost or stolen with, it may be possible for others not only to obtain access to private financial information but to use the data to illegally access bank accounts, credit cards, etc. Quick intervention is extremely important to minimize problems for the taxpayer.

- ❖ Inform your volunteer supervisor about the situation
- ❖ **Call 1-800-424-2277**, ext 36021 or ext 36027 (during business hours), or 1-202-434-6021/6027 (after hours), immediately (within 24 hours) if **ANY** computer containing taxpayer data is lost or stolen.
- ❖ If the loss is the result of theft, call the local police to report the theft as soon as you realize what has happened.

**Computers lost, stolen, or damaged *without* taxpayer data residing on them:**

Even with reasonable care and security, AARP or IRS equipment may be stolen or lost in fire, flood, or other natural disasters. Should a loss of AARP or IRS equipment occur, the state TCS **must** be notified. Please tell your supervisor so he or she can get the information to the TCS. If your supervisor is unavailable, call 1-800-424-2277 ext 36021 or 36027 (during business hours), or 1-202-434-6021/6027 (after hours), and AARP Tax-Aide staff will make sure the appropriate notification is made.