Best Practices for Keeping Client Data Secure

In light of the continuing increase in identity theft cases, your clients could easily become victims. Clients trust that you are doing everything that you can to keep their information secure. As a CPA, you have access to some of the most sensitive personal client data. If you do not already have a security plan, you should consider putting one in place immediately.

There are Federal and state laws that penalize breaches of private information. Having a secure policy in place to prevent identity theft will not only help to prevent breaches of client information, but may help defend you/your business if you ever have a breach of security. The penalties, in some cases, have been quite severe.

To help get you started, the following is a list of best practices that can be implemented as part of your overall security plan.

- **Clean desk policy** – This sounds like a policy to keep your office looking nice, but that is just an added bonus. This policy requires all paper and removable media (CD, USB, etc.) with client information be locked up every night when you close the office. It requires locking file cabinets in every staff office, a locked paper file room and locked shred bins. The last one to leave for the night makes a quick run through the office to make sure all the offices have been cleaned up and file cabinets/doors are locked. At first, implementing this policy can be difficult, but after a few days, it will just be part of your staff's routine. Another added bonus is less paper, as staff will be more careful about printing if they are going to have to lock up files every night.

- **Secure portals** – Having portals on your secure website for your clients' information has many benefits. Clients will have access to the information you choose to put in their portal when they need it. Some portal programs allow clients to upload their information and transfer it to you. You should already have a policy in place that no sensitive client information can be sent via email unencrypted. However, consider going one step further and not allow any sensitive information be sent via email. Breaking the encryption on a password-protected PDF file is not very difficult. Having portals can also lead to less paper, as providing a paper copy of tax returns is no longer necessary.

- **Hardware security** – You should always have updated anti-virus software on all machines/networks, along with the appropriate computer firewalls. Do not be your own IT professional. Hire a reputable company/IT expert to make sure your digital information is secure. Other steps you can take to increase the security of the data on your hardware include:

    - Have policies in place that prevent staff from saving client data to local computer drives.
    - Encrypt hard drive information on your local machines (Windows 7 has an optional BitLocker Drive Encryption feature).
    - Properly dispose of old computer equipment and also consider other hardware such as printers, copiers, and fax machines.
    - Install a camera monitoring system in the office, specifically capturing traffic through the front door and all file areas containing client information. The price of monitoring equipment is affordable and you can easily monitor activity through the internet when you are away from the office. Certain camera security systems even send an email alert when motion is detected in a room during a custom period of time set by the user.

- **Reputable third-party providers** – You should only use reputable third-party providers of services including janitors, tax software, SAAS providers, and IT support. Make sure to do your own vetting for any provider who could or will have access to your client information. Among some of the steps you can take are:
    - Ask for and check references.
    - Inquire if the service provider is bonded.
    - Check if the service provider's website is secure and if they have successfully completed an SSAE 16 Type II examination or SAS 70 audit.

- **Disclosure authorizations** – Before disclosing client information to a third party, you are required under Federal law to have a disclosure authorization signed by your client. Keep a signed copy of the authorization in your file. It's important for your client to know who you provide his or her information to, and it protects you later, should a dispute arise between your client and the third party.
    - Stamp all of your client's information as "confidential."
    - Include a disclosure indicating that you are sending the information per the request of your client and the information must be kept secure.
    - When emailing information, request that the recipient let you know if he or she is not the intended party.
    - When faxing information, verify that the information got to the intended person.
    - TIP: Where possible, arrange for your client to provide the information to the third party. For example, if a lender needs a copy of your client's tax return, provide the return to your client to submit it to his or her lender. If you do not actually provide the information to the third party, no disclosure authorization is needed.

- **E-filing** – E-filing tax returns not only saves on paper and postage, but it means that you don't have to put a tax return in the mail and worry about it being lost or stolen. As an added bonus, you may be the first to know if your client was subjected to certain types of tax-related identity theft, as you will get a rejection code when you attempt to e-file the return. Even though you have to be the bearer of bad news in this case, your client will appreciate you helping them through the process.

- **Payment Card Industry (PCI) compliance** – If you are accepting credit cards for payment of your services, you are required to comply with the PCI data security standards. By complying with these standards, you will not only be protecting the credit card information of your clients, but you may also be eligible to receive a discount from your credit card service provider.

- **Environment of privacy** – Within your organization, an environment of strict privacy of client information should be upheld as one of your top priorities. The policy, at a minimum, should restrict staff from discussing client information with his or her spouse or other family members, former employees, hairdresser, etc. It should also state that even discussing clients with other staff in public, using nicknames or client initials, is also forbidden. This policy should be signed by every staff member on his or her first day or work and staff should be reminded of it on a regular basis.

- **Employee training** – All employees should be provided regular training on data security, which should include information on phishing emails, social engineering, and other ways unauthorized users could get access to your client information. If you employ all of the above securities and one staff member clicks on a phishing email, he or she could infect your whole network without even knowing it. Training will teach staff to be vigilant guardians of your client information.

- **Terminated employees** – Have a policy in place regarding access to electronic files, computers and networks for terminated/departed employees. All access to secure data, networks, firm website, etc., should end upon an employee's departure.

- **Internet restriction** – Consider unplugging the internet from computers that do not need that connectivity. For example, have computers dedicated entirely to internet research that do not have access to client data. Also, keeping internet off of staff computers can avoid the temptation to check private emails, search for non-work-related items, etc.

- **Lead from the top** – This is true of every policy in your firm. If the top management doesn't follow the policies, neither will any of the staff.

Don't wait for your clients to come asking what you are doing to keep their information secure. Instead, be proactive and ready to show them the procedures and policies you already have in place.