Privacy, Confidentiality, and Electronic Communications

CPAs have long recognized a responsibility to clients not to disclose confidential information received during a professional service engagement without a client's specific consent. This responsibility is embodied in the AICPA's *Code of Professional Conduct.* State accountancy laws and rules (including the *Uniform Accountancy Act*), federal and state tax laws, and other regulatory guidelines also impose confidentiality requirements.

Confidentiality concerns the protection of both business and personal data from discovery by unauthorized entities or individuals. *Privacy,* a subset of confidentiality,concerns only the protection of personal data. While CPAs have always had a duty to maintain client confidentiality, federal and state laws governing privacy protection have imposed, directly or indirectly, additional requirements on the practicing CPA.

For example, at the federal level, the *Safeguards Rule*, issued by the Federal Trade Commission (FTC) in connection with passage of the (GLB Act)*,* imposes a duty on all businesses, regardless of size, that are "significantly engaged" in providing financial products or services[1] to develop a written information security plan. Professional preparers of tax returns for individuals fall within this category*.* More recently, the *Health Information Technology for Economic and Clinical Health Act* (the HITECH Act) contains amendments to the *Health Insurance Portability and Accountability Act* (HIPAA) which subject *business associates*[2] to the same HIPAA security and privacy rules as their health care clients. CPA firms with access to *individually identifiable health information*[3], such as those which process patient billing records, may fall within this category.

Spurred on by a growing e-commerce market place, the use of cyberspace as a medium for the transmission and storage of personal and business information (i.e., client portals and cloud computing), acts of identity and credit theft, privacy and confidentiality concerns are continuing "hot" topics.

The AICPA has responded to e-commerce businesses seeking to provide assurance to their customers about on-line practices and controls with the development and introduction of *WebTrust* services. The AICPA and the Canadian Institute of Chartered Accountants formed the AICPA/CICA Privacy Task Force, which developed the Generally Accepted Privacy Principles (GAPP). These can be used by CPAs to assist clients in designing and implementing sound privacy practices and policies. But what should CPAs be doing in their own firms to protect the privacy and confidentiality of client and firm information? For starters, consider the following:

- *Review relevant laws, regulations, rules and professional standards concerning privacy.* As referenced above, laws are continuing to be drafted and implemented in many jurisdictions that impose specific responsibilities on businesses to protect the privacy and confidentiality of client information. In some cases professionals may be required to initiate or refrain from a specific action to comply. Consult with an attorney regarding these laws, regulations and rules prior to deciding how to proceed in protecting client privacy and confidentiality.
- *Develop and implement a written privacy and confidentiality policy for the firm.* The policy should define the types of information the firm collects and the security measures it employs to ensure the information is used and retained only as intended by the client, employee, etc. In addition, the policy should specifically describe the firm's policies and practices relating to the use of software and electronic devices (i.e., social media or instant messaging applications, e-mail, laptop computers, personal digital assistants, smartphones, etc.) for communicating with clients and others and relating to electronic data storage along with the applicable security measures employed. Firms that have networked computer systems or allow employees to use their personal computers or electronic devices to render services should also consider consulting with an information technology security specialist in developing the policy.
- *Inform employees about the contents of the privacy and confidentiality policy and conduct training to help employees meet their specific responsibilities in carrying out the policy.*
- *Obtain the client's written consent regarding the firm's use of communication software and electronic devices to transmit personal or confidential information.* Firms that host client data via an Internet-based portal should obtain a signed client agreement for use of this as well.
- *After implementing a privacy and confidentiality policy and related procedures, periodically monitor that the established procedures are being followed and operating as intended.*

E-mail and instant messaging are common methods for communicating in today's business environment. Despite their widespread use and efforts by many to improve Internet and electronic security, using these technologies for normal communications continues to present the risk that information may be intercepted and used by unauthorized persons. Once data is transmitted electronically, the firm generally has no control over its possible interception and unauthorized use.

Firms should inform clients about their intended use of communication software and electronic devices, and obtain clients' written consent to their use. Consent can be included

as part an engagement letter. The following is an example of wording that could be included:

"In the interest of facilitating our services to your company, we communicate by use of electronic devices and send data over the Internet, including but not limited to electronic mail. Such communications may include information that is confidential to your company. Our firm employs measures in the use of computer technology designed to maintain data security. While we will use reasonable efforts to keep such communications secure in accordance with our obligations under applicable laws and professional standards, you recognize and accept that we have no control over the unauthorized interception of these communications once they have been sent, and you consent to our use of these electronic devices during this engagement."

Firms may also communicate with non-clients using electronic mail. In such instances, the firm has no intention of making any communications the equivalent of a professional engagement. In these situations, the firm may want to include a disclaimer of such as part of the transmission. An example of disclaimer wording that may be used follows:

"The content of this transmission does not constitute a professional service. Always consult with a competent professional service provider for advice on tax, accounting and other financial matters specific to your situation. If you wish to engage our firm for this purpose, please contact our office."

E-mails should include a statement directed to those who may receive a message in error. This statement is intended to protect the sender and minimize the risk that confidential information will be used inappropriately. Such a statement could read as follows:

"This message contains information that may be confidential and privileged. Unless you are the addressee (or authorized to receive for the addressee), you may not use, copy, print or disclose to anyone the message or any information contained in the message. If you have received this e-mail in error, please advise the sender by reply and delete the message. Thank you."

Firms interested in including any of the above examples in their communications should tailor the language used to their specific situation and consult with an attorney regarding appropriate wording for disclosures and disclaimers before using them.

Whether messages are sent over the Internet or merely over a firm's internal network, e-mail is a particularly sensitive tool with respect to privacy and confidentiality concerns. E-mails are easy to send to both single and multiple recipients and, once sent, the author loses control over further potential distribution by the original recipient. Further, the seeming indestructibility of e-mails poses the added risk of potential unintended use and discovery of the contents. Merely hitting the "delete" key on a computer, PDA, or smart phone does not irretrievably destroy an e-mail message.

Whether a firm has a single computer or a large network, information technology specialists should be consulted on e-mail security issues including, for example:

- System safeguards such as system design, backup measures, firewalls, virus protection, and message encryption.
- Controls over both in-office and out-of-office use of e-mail systems.
- Protection of firm and employee-owned computers and other electronic devices used for business from unauthorized access and installation of unauthorized software.
- Password protection and other security devices.

Maintaining client privacy and confidentiality is an important professional and legal responsibility. Protect your clients *and* your firm by establishing and following a written privacy and confidentiality policy. Once in place, monitor compliance as a routine element of your firm's quality control.

Resources:

- AICPA Information Technology Center (includes AICPA Privacy/Data Protection Resources) at: http://www.aicpa.org/INTERESTAREAS/INFORMATIONTECHNOLOGY/RESOURCES/Pages/default.aspx
- Federal Trade Commission Safeguards Rule Resources at: http://www.ftc.gov/privacy/glbact/glbsub1.htm
- U.S. Department of Health and Human Services Health Information Privacy Resources at: http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/index.html
- WebTrust at: http://www.webtrust.org

April 2011

CNA Accountants Professional Liability, CNA Plaza, Chicago, Illinois 60604

This information is produced and presented by CNA, which is solely responsible for its content.

The purpose of this article is to provide information, rather than advice or opinion. It is accurate to the best of the author's knowledge as of the date of the article. Accordingly, this article should not be viewed as a substitute for the guidance and recommendations of a retained professional. In addition, CNA does not endorse any coverages, systems, processes or protocols addressed herein unless they are produced or created by CNA.

Any references to non-CNA websites are provided solely for convenience, and CNA disclaims any responsibility with respect to such websites.

To the extent this article contains any examples, please note that they are for illustrative purposes only and any similarity to actual individuals, entities, places or situations is unintentional and purely coincidental. In addition, any examples, including the sample letter, are not intended to establish any standards of care, to serve as legal advice appropriate for any particular factual situations, or to provide an acknowledgement that any given factual situation is covered under any CNA insurance policy. Please remember that only the relevant insurance policy can provide the actual terms, coverages, amounts, conditions and exclusions for an insured. All CNA products and services may not be available in all states and may be subject to change without notice.

IRS Circular 230 Notice: The discussion of U.S. federal tax law and references to any resources in this material are not intended to: (a) be used or relied upon by any taxpayer for the purpose of avoiding any federal tax penalties; (b) promote, market or recommend any products and/or services except to the extent expressly stated otherwise; or (c) be considered except in consultation with a qualified independent tax advisor who can address a taxpayer's particular circumstances.

1. *Financial institutions*, as defined by the GLB Act;
see http://business.ftc.gov/documents/bus53-brief-financial-privacy-requirements-gramm-leach-bliley-act

2. As defined by HIPAA; see http://www.hhs.gov/ocr/privacy/

3. Ibid.