Published in: JOURNAL OF ACCOUNTANCY

AICPA® Professional Liability SPOTLIGHT

June 2015

Due diligence with CPA firm subcontractors

By Joseph Wolfe

CPA firms often use subcontractors to help provide payroll, tax, accounting, and audit services or to provide administrative support to the firm. In the course of rendering these services, subcontractors may obtain access to a vast amount of confidential client data. Examples of subcontractors include part-time help hired during busy season, other accounting firms assisting with tax return preparation, or even companies that provide mailroom or office cleaning services.

Individuals with access to large amounts of electronic data pertaining to clients and the firm can create havoc in minutes. The legal and professional responsibilities of a CPA firm related to privacy of client data also extend to the actions of their subcontractors. Consider this related story involving a privacy breach by a subcontractor in the health care industry.

Example. GMR Transcription Services (GMR) employed a subcontractor named Fedtrans to transcribe audio files received from GMR's customers. Fedtrans downloaded the files from GMR's network, transcribed them, and uploaded the transcripts back to the network. Because of an error by the subcontractor, the transcripts were indexed by a major internet search engine and became publicly available to anyone using the search engine. The files contained detailed notes from medical examinations about psychiatric disorders, alcohol use, and other confidential patient information. The Federal Trade Commission (FTC) conducted an investigation and charged GMR with failing to employ reasonable and appropriate measures to prevent unauthorized access to personal information by the subcontractor. The terms of the settlement with the FTC required GMR to submit biennial assessments and reports on its information security program for 20 years. (Federal Trade Commission, "Provider of Medical Transcript Services Settles FTC Charges That It Failed to Adequately Protect Consumers' Personal Information," available at ftc.gov.)

MORE THAN A TECHNOLOGY ISSUE

Typically, unauthorized disclosure of confidential client data by a subcontractor relates to the activities of its employees rather than a rogue act by an unknown third-party hacker. Subcontractors with inadequate controls over access to data present elevated risk to CPA firms. A breach may arise from unintentional and careless mistakes, as well as from intentional acts by subcontractor employees.

Understanding subcontractors' restrictions on access to electronic data and instituting redundant systems to limit access represent critical factors in conducting due diligence. However, due diligence also demands CPA firms evaluate the privacy and security practices of potential subcontractors. In addition, a CPA firm should review each subcontractor's protocol in screening, training, and monitoring its workers with access to confidential client data, as well as its physical security safeguards. The CPA firm also should review indemnification, data breach protocol, and insurance coverage provisions in contracts with subcontractors.

PROFESSIONAL AND LEGAL OBLIGATIONS

CPA firms are subject to privacy and security obligations under AICPA *Professional Standards*, state boards of accountancy rules, and the Internal Revenue Code (IRC). The AICPA *Code of Professional Conduct* addresses the use of third-party service providers in ET Sections 1.150.040, 1.300.040, and 1.700.040. ET Section 1.700.040 indicates that in the absence of obtaining specific consent from the client before disclosing confidential information to the provider, the CPA should enter into a contractual agreement with any subcontractor addressing procedures to prevent the unauthorized release of confidential information to others.

IRC Sec. 7216 imposes misdemeanor criminal penalties on tax return preparers who disclose or improperly use taxpayer information. The regulations and IRS guidance require tax return preparers to obtain specific taxpayer consent prior to disclosing tax return information to subcontractors (and any other third parties) and require the use of an "adequate data protection safeguard" when taxpayer information is sent to a return preparer located outside the United States (Regs. Sec. 301.7216-3 and Rev. Proc. 2013-14, §5, as modified by Rev. Proc. 2013-19).

CPA firms and their subcontractors also must comply with applicable privacy laws, such as the FTC Safeguards Rule, the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Health Information Technology for Economic and Clinical Health Act (the HITECH Act), and state security breach notification laws. (For more information, see "Professional Liability Spotlight: A Breach of Client Data: Risks to CPA Firms," *JofA*, Aug. 2013, page 18, and "How Health Care Data Security Rules May Affect You," *JofA*, Jan. 2015, page 54.)

Responsibility for compliance with these professional and legal obligations extends to the privacy and security practices of subcontractors.

So, what are CPA firms to do? Relying on the good faith of subcontractors is not a viable solution. Rather, a CPA firm should consider implementing appropriate risk mitigation strategies.

SUBCONTRACTOR SCREENING, TRAINING, AND MONITORING PRACTICES

CPAs should understand how subcontractors screen, train, and monitor workers who have access to confidential client data.

- Does the subcontractor use a third-party company to perform background checks or have a written policy on screening? Background screening companies vary widely in experience, qualifications, and services provided. Review the subcontractor's screening policy, if applicable. While confidential client information is vulnerable to exploitation for profit, employers are restricted in asking about criminal convictions in the hiring process. (For more information, see "Professional Liability Spotlight: Criminal Background Checks Can't Remain in the Background Anymore," *JofA*, April 2013, page 16.)
- Review the subcontractor's written employee policies and training materials on maintaining confidentiality. Training materials should encompass ethical conduct, as well as a response when unethical actions or behaviors by others are observed. An "open door" policy to encourage disclosure of concerns regarding employee behavior or misconduct without fear of retaliation is desirable.
- Ask about the subcontractor's controls over physical security, and processes to monitor employee behaviors and actions.

If these issues raise concerns, consider how to best mitigate the risks. Some techniques are within the direct control of the CPA firm, such as maintaining a "clean desk" policy to prevent unauthorized access to records by cleaning service employees. Other risks may be mitigated through further action by the subcontractor. CPAs should advise subcontractors to consult with their attorneys regarding employee screening and monitoring processes.

ADDRESSING SUBCONTRACTOR PRIVACY AND SECURITY POLICIES

CPA firms also should review subcontractors' privacy and security policies. While small subcontractors may not have written policies, CPAs should confirm that prospective subcontractors maintain adequate controls over these matters. Due diligence should be performed when seeking services from new subcontractors and updated at regular intervals in ongoing relationships.

An excellent related resource is the Generally Accepted Privacy Principles (GAPP) issued by the AICPA and the Chartered Professional Accountants of Canada. The business version of these 10 Generally Accepted Privacy Principles is available at aicpa.org. Consider using these privacy principles to evaluate and recommend improvements to subcontractors' policies and procedures.

CONTRACTS AND INSURANCE COVERAGE

Enter into a written contract with the subcontractor that addresses privacy and security policies, indemnification, data breach protocol, and insurance coverage, and have your attorney review the contract prior to execution. Among other issues, it should address:

- Representations made by the subcontractor regarding privacy and security practices;
- The subcontractor's obligation to maintain privacy and security;
- The obligation to promptly inform the CPA firm in writing in the event that a breach of privacy occurs;
- Indemnification of the CPA firm in the event of a security breach; and
- Minimum limits of liability insurance required.

Contractual provisions may be important in defending a CPA firm's actions in the event of a regulatory investigation or lawsuit related to a subcontractor's privacy breach.

Liability insurance for the actions of subcontractors should also be evaluated, including exposures related to privacy breaches in handling CPA firm data, working on the premises of the CPA firm or its clients, and traveling to and from these locations. Investigate the application of insurance coverage under CPA firm policies to the acts of subcontractors. Some policies extend coverage to the acts of subcontractors, while others do not. CPA firms should consult with their attorney and insurance agent or broker regarding these matters.

FINAL THOUGHTS

While the above items are good considerations to help evaluate a subcontractor's privacy and confidentiality policies, what would happen if a client asked your CPA firm similar questions? Now is an excellent time to review and update the firm's processes to protect confidential client data, train employees, and understand how insurance coverage may apply in the event of a data breach.

Joseph Wolfe *(joseph.wolfe@cna.com) is a risk control consulting director at CNA.*