Published in: JOURNAL OF ACCOUNTANCY

AICPA
Member Insurance Programs

PROFESSIONAL LIABILITY SPOTLIGHT

March 2019

Dealing with subpoena requests for digital data

By H. Steven Vogel, Esq., and Deborah K. Rood, CPA

A CPA firm received a subpoena for the production of its documents related to an S corporation tax return where one shareholder alleged criminal activity on the part of the other shareholder. The firm contacted its professional liability insurer, which retained an attorney to help the firm properly respond. The attorney requested a copy of the firm's record retention policy (RRP) and the relevant documents. After providing documents to respond to the subpoena, the CPA firm considered the matter closed.

Or so it thought.

After reviewing the documents that were produced, the plaintiff's attorney believed the firm's production was incomplete and that portions of an email string potentially were missing. Additional discovery found numerous emails and text messages stored on a partner's personal home computer and mobile phone that were missed in the initial response to the subpoena.

With this additional information, the plaintiff's attorney turned his attention to the CPA firm, believing the CPA firm was not disclosing information about the shareholder's potentially criminal activity. After five years of unsuccessful pursuit of this theory, the matter was dismissed, but not before the CPA firm lost hundreds of hours of billable time and incurred tens of thousands of dollars in legal fees responding to what first appeared to be a "simple" subpoena.

What went wrong? How did the firm miss several key electronic documents when formulating its initial response to the subpoena?

The firm's RRP did not address all sources of "electronically stored information" (ESI). Therefore, the firm's response failed to include items stored on personal devices. The proliferation of ESI and the multitude of places where it may be stored leave an electronic data trail with no true road map for a CPA firm to follow when producing such information. Consequently, CPA firms should recognize the importance of evaluating their record storage procedures and consider modifying their existing RRP to address ESI.

DEFINITIONS

To start, terminology related to ESI should be defined:

- ESI: Information created, manipulated, communicated, stored, and/or best used in digital form, requiring the use of computer hardware and software.
- Electronic storage media: Any and all electronic devices that can be used to store data, including internal and external hard drives, CDs, DVDs, USB drives, Zip disks, magnetic tapes, SD cards, copy machines, cellphones, "smart" appliances, and more. While a firm may opt to expressly prohibit the use of personal devices to store firm data, the definition of ESI should encompass all relevant information on both business and personal devices. Thus, employees are fully aware that all business data, irrespective of where it is stored, is subject to the firm's RRP.
- Electronic discovery or e-discovery: This refers to any process by which electronic data are sought, secured, and searched with the intent of using them as evidence in a lawsuit, arbitration, or other alternative dispute resolution proceeding.
- Metadata: This has been described as "data about data." It describes the characteristics, origins, and use of electronic files.

HOW COULD ESI BE INVOLVED IN A PROFESSIONAL LIABILITY CLAIM?

Failure to comply with a subpoena or RRP

Subpoenas often include specific protocols for the production of ESI. Therefore, the firm's RRP should be reviewed in conjunction with the protocol referenced in a subpoena to ensure proper and efficient compliance with both. In the event of a claim, noncompliance with a firm's RRP may make the CPA firm appear dishonest or that it is trying to conceal information from the plaintiff as in the example above. The failure to follow subpoena protocol also may result in additional costs to search for, and produce, the requested documents. The firm could potentially be charged with contempt of court for failing to comply with the subpoena.

E-discovery preservation concerns

Proper maintenance and preservation of ESI is critically important and closely related to the RRP. Establishing a protocol for a firmwide litigation hold is also important when a firm receives a subpoena or is threatened with a lawsuit. A "litigation hold" permits the firm to halt all changes to and deletion of records in order to preserve them for discovery. Any alteration to electronic data, whether intentional or unintentional, will be recorded in the metadata of a file and cannot be erased.

Continued.

The failure to execute a required litigation hold protocol or to prevent the alteration of any ESI, including its metadata, following receipt of a subpoena or the threat of litigation may result in charges of spoliation of evidence. Similar to the failure to comply with subpoena protocol, monetary and other court sanctions may be imposed if there is evidence that ESI was not maintained or produced, or was altered.

SO WHAT SHOULD YOU DO?

Establish an RRP

Every firm should have and comply with its RRP. If the firm does not currently have an RRP, it should hire an attorney familiar with services provided by the firm, professional standards, and federal and state laws to assist it in creating an RRP.

Ensure the RRP addresses ESI

The RRP should include protocols for the maintenance and preservation of ESI. The RRP should address the time frame for saving emails as well as other documents with specific reference to statutes of limitation contained in the Internal Revenue Code or state law.

In addition, the RRP should address and prohibit the alteration of ESI following receipt of a subpoena or other litigation hold triggering event, such as the receipt of a litigation summons or a request from an attorney to secure records. How the existence and implementation of a litigation hold is communicated to firm owners and employees should also be addressed.

ESI-related items to be considered in an RRP include but are not limited to: (1) designation of an individual to oversee the legal hold process and monitor the collection of ESI; (2) the locations of ESI; and (3) how ESI is to be retrieved including how to retrieve information from legacy systems.

ESI may never disappear from the server or other storage media

When you are required to search for and produce ESI, remember that it may exist on third-party websites, such as portals, remote servers, social media platforms, or commercial email sites as long as required by that organization's policy. It will be necessary to search for and produce relevant documents from these sites.

Firms should consider policies that identify acceptable uses of social media for substantive work-related matters. Ideally, firm members would have separate social media presences for personal and business purposes.

Address how ESI will be recovered in the event of a records request

Gone are the days when only one or two places must be searched when a subpoena arrives. Instead, every server, desktop, laptop, tablet, and smartphone — including backups for those devices — is a data repository that must be accounted for. Moreover, firms must ensure that the ESI continues to be readable. For example, if operating systems or software have changed, data may no longer be accessible.

H. Steven Vogel, Esq., *is a shareholder and attorney with Becker & Poliakoff PA.*
Deborah K. Rood, CPA, *is a risk control consulting director at CNA. For more information about this article, contact specialtyriskcontrol@cna.com.*

Continental Casualty Company, one of the CNA insurance companies, is the underwriter of the AICPA Professional Liability Insurance Program. Aon Insurance Services, the National Program Administrator for the AICPA Professional Liability Program, is available at ***800-221-3023 or visit cpai.com****.*

This article provides information, rather than advice or opinion. It is accurate to the best of the authors' knowledge as of the article date. This article should not be viewed as a substitute for recommendations of a retained professional. Such consultation is recommended in applying this material in any particular factual situations.

Examples are for illustrative purposes only and not intended to establish any standards of care, serve as legal advice, or acknowledge any given factual situation is covered under any CNA insurance policy. The relevant insurance policy provides actual terms, coverages, amounts, conditions, and exclusions for an insured. All products and services may not be available in all states and may be subject to change without notice.

CNA

Contact me to learn more about the
AICPA Professional Liability Program:
Name
Aon Affinity
1100 Virginia Drive, Suite 250
Fort Washington, PA 19034
t +1.xxx.xxx.xxxx
xxxxxx.xxxxx@aon.com | cpai.com

AON
Empower Results®