To AICPA members in public practice that perform ERISA employee benefit plan audits:

It has come to our attention that auditors of employee benefit plans are increasingly being asked by recordkeepers, third-party administrators (TPAs), and other service organizations to sign nondisclosure agreements, confidentiality agreements, business associate agreements, data protection agreements, and other types of agreements (collectively, NDAs or other agreements) that could, if adhered to, cause the auditor to violate professional standards, laws, or regulations and may place the auditor at risk if auditors agree to provisions with which they are unable to comply. The purpose of this letter is to highlight the possible risks and requirements auditors need to be aware of before entering into NDAs or other agreements.

**Background**

Many employee benefit plan sponsors use third-party service organizations such as recordkeepers, administrators, and TPAs (service organizations) to perform the recordkeeping or administration functions for their plan(s). These service organizations often use electronic sites or portals (collectively, portals) to maintain plan information for a plan sponsor that is relevant to the audit. Rather than downloading such information and providing it to the auditor, it is becoming increasingly common for plan sponsors to ask their auditors to access these portals directly. It is the plan sponsor's responsibility to provide the auditor with the necessary information to complete the audit without limitations.

To access information relevant to the audit that is maintained in the portal, auditors are often prompted to first accept the site's terms of use. It is important to understand that such terms may include NDAs or other agreements that compromise or otherwise limit the auditor's ability to perform an independent financial statement audit required by Title I of ERISA because they conflict with professional standards, laws, or regulations. In particular, certain provisions in NDAs or other agreements may cast doubt on the auditor's ability to rely on the information in the portal or may not appropriately recognize the auditor's obligations related to information included in audit documentation (or audit working papers). Auditors are already subject to requirements related to confidentiality of client information, which may serve the same purpose as an NDA with a third-party service organization.

The rules of the American Institute of Certified Public Accountants (AICPA) Professional Code of Conduct (the Code) require the auditor to maintain the confidentiality of information obtained in the course of performing the audit, including proprietary information of the client itself. Specifically, ET section 1.700.001.01 of the Code addresses the auditor's responsibility to obtain the client's specific consent for the disclosure of any confidential client information. Auditors are also subject to the security and privacy provisions of the Health Insurance Portability and Accountability Act (HIPAA) with respect to health claim information obtained during an audit of a health and welfare plan. Noncompliance with professional standards or HIPAA could result in potentially severe consequences to auditors.

In addition, it would appear that NDAs or other agreements may be in direct conflict with Department of Labor's (DOL) Rule 29 CFR §2520.107-1, *Use of electronic media for maintenance and retention of records,* which addresses the maintenance and retention of plan information through electronic format under sections 107 and 209 of ERISA. Among other things, it states that those requirements are satisfied when using electronic media if:

> The electronic recordkeeping system is not subject, in whole or in part, to any agreement or restriction that would, directly or indirectly, compromise or limit a person's ability to comply with any reporting and disclosure requirement or any other obligation under Title I of ERISA.

Prohibiting an auditor from obtaining or using information relevant to an audit, including information maintained in a service organization's portal, can result in a modified auditor's opinion, Form 5500 rejection, monetary penalties for the plan sponsor, and noncompliance with DOL Rule 29 CFR §2520.107-1 by the service organization.

**Examples of potential risks to auditors**

When seeking to access information that is relevant to the audit from service organization portals, we have seen NDAs or other agreements that include provisions that:

1. ***Require the auditor to maintain the confidentiality of all information obtained through the portal.***

In these provisions, confidentiality terms are often not presented. In some cases, auditors are required by professional standards, laws, or regulations to make audit working papers available for review by third parties. Examples include inspections by the DOL, the AICPA Peer Review and Professional Ethics programs, the Public Company Accounting Oversight Board (PCAOB), or state boards of accountancy. Under the Code, paragraph .05 of the Records Requests interpretation [ET sec. 1.400.200 of the Code] states:

> Members must comply with rules and regulations of authoritative bodies, such as the member's state board(s) of accountancy, when the member performs services for a client and is subject to the rules and regulations of such regulatory body.

As the rules and regulations of each of the aforementioned authoritative bodies require the auditor to make audit working papers available as part of their respective inspection programs, auditors would be unable to comply with provision # 1 while also complying with ET sec. 1.400.200 of the Code.

2. ***Prohibit the auditor from using any information obtained through the portal OR require the auditor to agree to download and print materials for personal non-commercial use only.***

If information relevant to the audit is maintained in the service organization portal, and the auditor is prohibited from using that information, such prohibition may cast doubt on the auditor's ability to rely on such information. The auditor would need to perform procedures to resolve such doubts. If the auditor is unable to resolve such doubts, the auditor would be responsible for evaluating the implications on the assessment of the relevant risks of misstatement, including the risk of fraud, and on the related nature, timing, and extent of other audit procedures. PCAOB AS 2810 Appendix C specifically indicates that denial of access to records, facilities, certain employees, customers, vendors, or others from whom audit evidence might be sought may affect the auditor's assessment of fraud risk.

Only by obtaining sufficient appropriate audit evidence through the performance of audit procedures (including, but not limited to, inquiry, analytical procedures, observation, inspection, and external confirmations) can the auditor express an unmodified opinion in accordance with auditing standards generally accepted in the United States ("GAAS") or PCAOB standards. Prohibiting the auditor from using information relevant to the audit may result in a scope limitation and a modified opinion or disclaimer of opinion on the financial statements as a whole, which might have a direct, adverse effect on the plan sponsor. For example, when an auditor issues a disclaimer of opinion and attaches it to a plan's annual Form 5500 filing, the DOL Employee Benefit Security Administration has indicated they may reject the filing, which may subject the plan sponsor to substantial monetary penalties.

3. ***Prohibit the auditor from copying, distributing, altering, or reproducing any information obtained through the portal.***

Under AU-C section 230, *Audit Documentation*, the auditor is required to prepare and retain audit documentation. Among other things, such audit documentation is required to be sufficient to enable an experienced auditor, having no previous connection with the audit, to understand

- the nature, timing, and extent of the audit procedures performed to comply with GAAS and applicable legal and regulatory requirements;
- the results of the audit procedures performed, and the audit evidence obtained; and
- significant findings or issues arising during the audit, the conclusions reached thereon, and significant professional judgments made in reaching those conclusions.

In doing so, when documenting the nature, timing, and extent of audit procedures performed in accordance with AU-C section 230, the auditor is required to record the identifying characteristics of the specific items or matters tested. Further, for audit procedures related to the inspection of significant contracts or agreements, the auditor is required to include abstracts or copies of those contracts or agreements, all of which may be obtained from the portal.

PCAOB standards also include specific and detailed requirements related to audit documentation and retention.

The audit documentation requirements are in direct conflict with provision # 3. Accordingly, auditors would be unable to comply with this provision while also complying with GAAS or PCAOB standards.

4. ***Require the auditor to destroy data obtained through the portal by a date that is earlier than the required audit documentation retention period.***

AU-C section 230 requires that the auditor not delete or discard audit documentation of any nature before the end of the specified retention period, which should not be shorter than five years from the report release date. Under PCAOB AS 1215, *Audit Documentation*, auditors must not delete or discard audit documentation after the documentation completion date. PCAOB AS 1215 also requires auditors to retain audit documentation for seven years from the auditor's report release date, unless a longer period of time is required by law. As these requirements are in direct conflict with provision #4, auditors would be unable to comply with this provision while also complying with AU-C section 230 or PCAOB AS 1215.

5. ***Require the auditor to notify the service organization directly of errors, inaccuracies, incompleteness, or other discrepancies in the information obtained from the portal.***

Notifying the service organization of errors, inaccuracies, incompleteness, or other discrepancies would be management's responsibility. If the auditor were to notify the service organization of these matters directly without plan management's agreement, the auditor would be viewed as assuming a management responsibility, which is prohibited by professional standards. ET section 1.295.030.01 of the Code states:

> If a member were to assume a management responsibility for an attest client, the management participation threat would be so significant that no safeguards could reduce the threat to an acceptable level and independence would be impaired.

Under ET section 1.200.001 of the Code, a member in public practice shall be independent in the performance of professional services as required by standards promulgated by bodies designated by Council, which includes the standards promulgated by the AICPA Auditing Standards Board (under which audits of employee benefit plans are conducted).

As such, auditors would be unable to comply with provision # 5 while also complying with the requirements of the Code.

6. ***Require the auditor to agree to access the information only for purposes specified in the license grant.***

In our experience, the license grants for accessing the information have not included audit services, making it impossible for the auditor to comply with this provision.

7. ***Require the auditor to indemnify and hold harmless the service organization from all claims of any nature arising from access to the information.***

In a February 2, 2024 article, *Indemnification Clauses in Client Agreements…the Saga Continues*, CAMICO Insurance, a major provider of professional and employment practices liability and risk management services for the accounting profession, outlines considerations for auditors when determining whether to sign an NDA or other agreement, including:

- taking great care in reviewing any such contracts or agreements;
- considering the worst possible scenario under the agreement and determining the level of risk the firm would be assuming;
- taking the time to understand all the implications of any legalese in the agreement to make an informed decision about terms and conditions that may pose a higher standard or greater liability to the firm; and
- making sure the firms is comfortable with the agreement and the expectations that will fall on the firm.

Because the auditor may be entering into such NDAs or other agreements solely for the purpose of accessing information directly from the service organization at the request of the employee benefit plan sponsor, the auditor may be accepting increased risk. It would be more appropriate for the employee benefit plan sponsor to take on the indemnity obligation towards the service organization in connection with any claims arising from the auditor's access to the information held by the service organization.

8. ***Require the auditor to agree to allow the service organization to monitor the auditor's access and use of the portal without notification to the auditor.***

This provision seems to be inappropriately invasive on the part of the service organization, especially given that the auditor is accessing the information for the purposes of performing an audit of the plan.

9. ***Indicate the terms and conditions of the NDA or other agreement may be changed at any time at the sole discretion of the service organization, without notice to portal users.***

Auditors do not regularly review for changes in NDAs or other agreements that would impact their ability to adhere to professional standards, laws, or regulations or the terms of such agreements. Such provisions can also increase risks to auditors.

**Recommendations**

As described in this letter, it is critical that auditors have unfettered access to the information needed in order to conduct an audit. Auditors are bound by ethical standards to keep client information confidential, which extends to information provided by service organizations.

It is management's responsibility to provide the auditor with the information required to perform the audit. As a reminder, AU-C section 210, *Terms of Engagement*, establishes the preconditions for an audit. Such preconditions include, among other things, obtaining the agreement of management that it acknowledges and understands its responsibility to provide the auditor with:

1) access to all information of which management is aware that is relevant to the preparation and fair presentation of the financial statements, such as records, documentation, and other matters;
2) additional information that the auditor may request from management for the purpose of the audit; and
3) unrestricted access to persons within the entity from whom the auditor determines it necessary to obtain audit evidence.

Auditors are encouraged to discuss the matters described herein with the plan sponsor and any other relevant parties involved in the audit and to suggest that the plan sponsor establish reasonable

procedural protections that provide practical alternatives to NDAs and other agreements or otherwise modifying standard provisions therein, such as:

- contracting with service organizations to ensure plan auditors have the information needed to conduct the audit without inappropriate limitations;
- requesting service organizations to modify standard provisions in NDAs and other agreements that are not intended to apply to auditors or otherwise negating the applicability of such provisions to auditors; or
- carefully identifying the data to be exchanged in the course of an audit and discussing alternatives for obtaining such data from service organizations.

Auditors may also consider discussing a workaround with the service organization, such as including language in the NDA or other agreement or in the audit package that notes that any provision that would cause the auditor to violate professional standards, laws, or regulations, or is otherwise impracticable to comply with, is unenforceable and does not apply to auditors.

Before signing an NDA or other agreement, auditors are strongly encouraged to discuss the terms with legal counsel to avoid a situation that would cause the auditor to violate the terms therein, as the auditor is required to comply with professional standards, laws, and regulations.

The information contained in this letter is provided for informational purposes only and is not to be construed as professional or legal advice on any subject matter.

For more information or if you have questions about the information in this letter, please contact the EBPAQC at EBPAQC@aicpa.org.

Sincerely on behalf of the EBPAQC Executive Committee,

Debbie Smith

Debbie Smith, CPA
Chair, AICPA Employee Benefit Plan Audit Quality Center Executive Committee