Employee Benefit Plan Audit Quality Center

Plan advisory

AICPA

Baden Gage & Schroeder LLC

The importance of retaining and protecting employee benefit plan records

The AICPA EBPAQC is a firm-based, volunteer membership center created with the goal of promoting quality employee benefit plan audits. Center members demonstrate their commitment to ERISA audit quality by joining and agreeing to adhere to the Center's membership requirements. EBPAQC member firms receive valuable ERISA audit and firm best practice tools and resources that are not available from any other source.

Visit the Center website at aicpa.org/EBPAQC to see a list of EBPAQC member firms and find other valuable tools prepared for plan sponsors and other stakeholders. For more information, contact the EBPAQC at ebpaqc@aicpa.org.

Contents

Introduction

The AICPA Employee Benefit Plan Audit Quality Center (EBPAQC) has prepared this advisory to provide you, the plan sponsor, administrator, or trustee, with an understanding of the importance of properly maintaining plan records, including retention requirements under the Employee Retirement Income Security Act of 1974 (ERISA) and your responsibilities for protecting personally identifiable and other sensitive information.

As a plan fiduciary, you are subject to certain responsibilities, including plan administration functions, such as maintaining the financial books and records of the plan — including protecting sensitive data — and filing a complete and accurate annual return/report for your plan (Form 5500, *Annual Return/Report of Employee Benefit Plan*).

This advisory describes ERISA and DOL record retention requirements, protecting personally identifiable information, the effect of inadequate records on audit scope and testing and the auditor's report, and the implications to the plan administrator for failure to properly retain records. The advisory also provides suggestions for best practices for record retention and data protection and additional resources.

The sponsor of the plan is the plan administrator under the law unless another individual, committee or group of individuals, or entity is specifically designated to assume this responsibility. The term plan administrator as used throughout this document refers to the party responsible for ensuring that accounting and record retention are appropriately performed, which may be the plan sponsor, third-party administrator or trustee.

What are plan records?

While there is no legal definition of what constitutes "plan records," the term generally is considered to include records that are legally required to be maintained under ERISA, DOL and IRS requirements, and for other purposes, such as the plan's independent financial statement audit. Plan records generally fall into *one* or *more* of four categories:

- Reporting and disclosure records include all of the forms filed with government agencies with respect to the plan.
- Benefits determination records include information necessary to determine benefits and eligibility for plan participation, and information related to plan and individual participant investment balances and benefit payments (including health and medical records for health and welfare plans).
- Accounting records include information that is used in the calculation, measurement, processing and communication of financial information about the plan. They may be used to confirm the accuracy and completeness of individual participant account and plan financial information, in financial statement preparation, and for determining plan tax qualification status.
- Plan governance records include documents that memorialize the plan administrator's fiduciary decisions.

Some plan records, such as the plan document and investment contracts, relate to the plan and its operations and are maintained at the plan level. Other plan records are specific to individual participants (e.g., benefit payments, participant elections and contributions) and are maintained at the participant level. Plan records can be prepared and maintained by the plan sponsor (legal, human resources, finance, payroll, and accounting), plan recordkeeper, plan administrator, investment custodian, or other third-parties, and may be in paper or electronic form.

Examples of plan records:

- The original signed and dated plan document and any amendments
- Summary plan description and summaries of material modifications
- The determination, advisory or opinion letter for the plan's tax qualification status
- Contracts with service organizations
- List of parties in interest, including trustee(s), custodians and others
- List of related parties
- Proof of the plan's fidelity bond
- Plan communications and notices to plan participants
- Regulatory filings with the DOL, IRS or PBGC (e.g., Form 5500, PBGC e-4010 filing; Form M-1 for MEWAs)
- Participant records (employee data), including date of birth, date of hire or rehire, breaks in service, date of termination, employee identification number, Social Security number, sex, marital/family status, employee classification, rate of pay or hours worked, other forms of compensation, support for hours worked
- Participant benefits statements
- Enrollment and election records including participant elections for salary deferral percentages and health and welfare option, investment direction, beneficiary designation, dependent information and distribution requests
- Payroll records used to determine eligibility and contributions
- Listing of contribution and distribution transactions
- Documents relating to plan loans, withdrawals and distributions
- Notarized spousal consents and waivers

- Nondiscrimination and coverage test results
- Officer and ownership history and familial relationships
- Information supporting reporting and disclosure in regulatory filings and the plan's financial statements
- Actuarial statements and valuations
- Plan accounting records
- Minutes, board resolutions, written plan policies and other governance documents.

Plan record retention

As part of their fiduciary responsibilities, it is important that plan administrators retain and maintain documents to support all plan activities, safeguard participant information, and comply with legal requirements (ERISA, DOL, and IRS), including IRS and DOL audits and examinations and financial statement audits. Records may be retained electronically or in paper format or both. Talk to your plan's ERISA counsel about your responsibility for retaining and maintaining plan records.

ERISA and DOL requirements

ERISA establishes requirements for record retention by the sponsor of a qualified plan in Sections 107 and 209. Section 107 of ERISA includes requirements for the retention of records used to support plan filings. Section 209 addresses maintaining participant records used to determine benefits.

ERISA Section 107. Section 107 of ERISA requires those plan records used to support filings, including the annual Form 5500, to be retained for at least six years from the filing date. For example, if a 12/31/X1 Form 5500 is filed on 10/15/X2 (the extended due date), the support records must be kept until 10/15/X8. Under ERISA section 107, the following documentation should be retained at least six years after the Form 5500 filing date (as discussed above), including, but not limited to:

- Copies of the Form 5500 (including all required schedules and attachments);
- Nondiscrimination and coverage test results;
- Required employee communications;
- Financial reports and supporting documentation;
- Evidence of Plan's fidelity bond;
- Corporate income-tax returns (to reconcile deductions)

ERISA Section 209. Section 209 of ERISA states that an employer must "maintain benefit records, *in accordance with such regulations as required by the DOL*, with respect to each of [its] employees sufficient to determine the benefits due or which may become due to such employees [emphasis added]." Proposed DOL regulations issued in 1980 state that participant benefit records must be retained "as long as a possibility exists that they might be relevant to a determination of the benefit entitlements of a participant or beneficiary." While the regulations were never finalized, the DOL has taken the position those record retention obligations apply beginning when the DOL issued its first set of proposed regulations under Section 209 on February 9, 1979, because employers were put on notice of the obligations. As such, plan sponsors should consider whether benefit plan records need to be maintained indefinitely.

Under ERISA Section 209, the records *used to determine the benefits that are or may become due to each employee* include, but are not limited to:

- Plan documents, and items related to the plan document including, adoption agreements, amendments, summaries of material modifications (SMMs), summary plan descriptions (SPDs), the most recent IRS determination letter, etc.
- Census data and support for such information including records that are used to determine eligibility, vesting, and calculated benefits (such as rates of pay, hours worked, deferral elections; employer contribution calculations)
- Participant account records and actuarial accrued benefit records
- Support and documentation relating to plan loans, withdrawals and distributions
- Board or administrative committee minutes and resolutions
- Trust documents

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) establishes standards for the electronic exchange, privacy and security of health information, for ERISA welfare benefit plans

DOL Rule 29 CFR § 2520.107-1, *Use of electronic media for maintenance and retention of records,* provides guidance on the retention of plan information through electronic format, as follows:

- The electronic recordkeeping system has reasonable controls to ensure the integrity, accuracy, authenticity and reliability of the records kept in electronic form;
- The electronic records are maintained in reasonable order and in a safe and accessible place, and in such manner as they may be readily inspected or examined;
- The electronic records are readily convertible into legible and readable paper copy as may be needed to satisfy reporting and disclosure requirements or any other obligation under Title I of ERISA;
- 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; and
- Adequate records management practices are established and implemented
- All electronic records must be legible and readable.

Generally, most original paper records may be disposed of any time after they are transferred to an electronic recordkeeping system that complies with the requirements of the DOL. However, plan administrators should be aware that original paper records may need to be retained for audit purposes.

IRS requirements

IRS Revenue Procedure 98–25 (revenue procedure) provides taxpayers, including employee benefit plans, with comprehensive guidance on requirements for maintaining and providing IRS access to electronic tax records. It specifies basic requirements in cases where a plan's records are maintained within an Automatic Data Processing system (ADP). The revenue procedure requires that:

- Plans retain electronic, or ''machine-sensible'' records, ''so long as their contents may become material to the administration of the internal revenue laws.'' Such materiality would continue at least until the period of limitations, including extensions, expires for each tax year. The Revenue Procedure notes that in certain situations, records should be kept for a longer period of time.
- The machine-sensible records provide sufficient information to support and verify entries made on the taxpayer's return and to determine the correct tax liability. The Revenue Procedure specifies how the plan may meet this requirement.
- All machine-sensible records required to be retained by the revenue procedure be made available to the IRS upon request and must be capable of being processed.

The revenue procedure also requires that the plan maintain documentation of the business processes that create, modify and maintain records; support and verify entries made on the plan's return; and evidence the authenticity and integrity of the plan's records, and includes details about how this requirement may be met.

The revenue procedure also requires the plan to promptly notify the IRS if any machine-sensible records are lost, stolen, destroyed, damaged or otherwise

no longer capable of being processed, or are found to be incomplete or materially inaccurate. The notice must identify the affected records and include a plan that describes how, and in what timeframe, the plan proposes to replace or restore the affected records in a way that assures that they will be capable of being processed.

The revenue procedure specifies that a taxpayer's use of a third-party service organization (e.g., custodial or management services) in respect of machine-sensible records does not relieve the taxpayer of its recordkeeping obligations and responsibilities.

Best practices for plan record retention

As discussed above, ERISA requires plan sponsors to retain broad categories of records related to meeting its fiduciary responsibilities. To do so, it is important that a plan sponsor understand the applicable rules and establish best practices for ensuring adequate record retention, including:

- *Establishing a written record retention policy governing how the organization periodically reviews, updates, preserves, and discards documents related to plan administration.* It should be approved by ERISA counsel or those charged with governance over the plan to ensure that federal and state retention laws are being considered and adhered to. When service organizations (e.g., recordkeeper, investment custodian) maintain plan records, the plan administrator needs to understand the retention policies of those service organizations for plan records they prepare and/or maintain. **Reminder — The use of a service organization does not alleviate the plan sponsor's responsibilities to retain adequate records.** Some general types of records that should be addressed as a part of any policy include:
  - Employer remittances and contribution reports
  - Benefit claims, benefit applications and supporting information
  - Vendor invoices, billings and contracts
  - Plan documents including the trust, Summary Plan Description, and related amendments and modifications
  - Employment-related records, including payroll records
  - Receipts and proof of disbursements, bank and investment statements, and loan documents, if applicable
  - Electronic data including emails and scanned documents
  - Board of Trustee minutes, budgets, financial statements and annual reports/tax returns

- *Monitoring compliance with the written record retention policy* — If the plan uses service organizations, the plan administrator should also monitor the service organizations' compliance with their respective retention policies.
- *Categorizing and documenting your plan records* — Data should be organized such that it can be easily and readily retrieved. Document the type of record, a brief description of the type of record, and the category to which records of this type belong. Records in the same category often have the same retention periods and might require similar treatment in other ways.
- *Maintaining important participant records indefinitely* — Because ERISA Section 209 does not provide a specific period of time for retaining participant-level records such as demographic information, compensation and elections sufficient to determine benefits due, these records should be kept for an indefinite period of time in a format that is easily retrieved to ensure they are available upon request by the participant or auditor in case of an audit.
- *Maintaining necessary paper records* — If electronic records don't establish a substitute or duplicate record of the paper records from which they are transferred under the terms of the plan or applicable federal or state law, the original records should not be discarded.

Protecting personally identifiable and other sensitive information

Data protection: Information security, confidentiality and privacy

Information security pertains to the safeguarding of an entity's data, whether or not it is personal or confidential. Confidential information is that which an entity or individual wishes not to make public. Privacy is the relationship between the collection, use, retention, disclosure and disposal of "personal information," and the legal and regulatory issues that surround these activities. Privacy *only* involves personal information; it does not apply to other information that may be confidential. Privacy concerns exist wherever personal information is collected or stored, whether in electronic form or otherwise, and any time it is sent or disclosed to a third party.

Plan administrators are required to make sure that the plan complies with ERISA, including HIPAA, which provides specific requirements for protecting protected health information (PHI). ERISA does not specifically address whether or how plans should protect personally identifiable information (PII). However, doing nothing to address privacy and security concerns in the current environment is inconsistent with ERISA fiduciary standards. State laws may also require consideration, and service organizations and individuals or entities that provide professional services to the plan may be subject to other non-ERISA laws that apply to PII. Discretionary selection of a service organization and hiring individuals or entities that provide professional services to the plan are fiduciary functions; personal information should not be shared with those providers that do not have in place the appropriate industry-standard safeguards to protect such information. Talk to your plan's ERISA counsel about your responsibility for protecting PII and other sensitive information, including plan records that are not in your possession.

PII

PII is information that can be used to distinguish or trace an individual's identity, such as their name, Social Security number (SSN), biometric records, etc., alone, or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. PII can be sensitive or non-sensitive. In some cases, PII can be anonymized by removing certain information so that the individuals whom the data describe can no longer be identified.

PII information can be maintained in either paper, electronic, or other media, and could be maintained by a plan sponsor or their service organizations. Some records that may contain PII include payroll records, human resource files, enrollment and election forms, plan compliance testing results, recordkeeping reports, and census files.

PHI — HIPAA indicates there are 17 health data elements referred to as "individually identifiable health information." When some or all of those data elements are used in conjunction with the name of the individual, that data is referred to as PHI.

Sensitive data — PHI and other data elements such as government identifiers or wage information are sometimes also referred to as "sensitive" indicating that additional measures should be taken either before the data is used or when the data is processed. For example, when using health data, measures can be taken to mask or truncate any health identifiers and to remove the patient's name from the data set.

Sensitive personal information includes, but is not limited to, data such as full name, SSN (both full and partial numbers are considered personal information, which means that the use of the last four digits only does not eliminate all privacy concerns), driver's license number, mailing address, credit-card information, passport information and financial information.

Non-sensitive or indirect PII — Non-sensitive or indirect PII is easily accessible from sources such as phone books, the internet, and corporate directories. ZIP code, race, gender and date of birth are all quasi-identifiers. Non-sensitive information is linkable, meaning that, when used with other non-sensitive linkable information, can reveal the identity of an individual.

Before agreeing to provide access to PII, some third-party service organizations require the plan administrator and auditor to sign confidentiality agreements or nondisclosure agreements (NDAs). Plan administrators should be aware that such agreements place both the plan administrator and the plan auditor in a difficult position. The information the service organization holds is essential to a plan administrator in meeting its regulatory and reporting requirements. If the service organization does not provide the plan administrator with the information requested by the auditor, it could adversely affect the plan administrator's ability to meet its fiduciary responsibility with respect to filing the plan's annual Form 5500. Withholding such information could constitute a restriction on the scope of the audit and, therefore, require a modification of the auditors' report and a disclaimer of opinion on the plan's financial statements. In such cases where a disclaimer is issued, the DOL likely would reject the filing, and the plan sponsor may be subject to substantial monetary penalties. See further discussion in the *Plan accounting records and the financial statement audit* section on page 21.

In addition, some NDAs include clauses that request the auditor to hold the client harmless, which could contradict provisions in the engagement letter between the auditor and the plan administrator. The plan administrator agrees to provide the auditor access to all books, records, and information necessary to conduct its audit of the plan financial statements. If the service organization has the ability to withhold plan records from the auditor, the auditor may not be able to rely on the plan administrator's assertions that the auditor has been provided access to all the books, records, and information necessary to fulfill his or her responsibilities.

In some instances, auditors are required by law to make audit workpapers available for review by third parties, making it impossible to comply with certain provisions of NDA agreements. However, auditors already are subject to strict professional standards that require them to maintain confidentiality of information obtained in the course of performing the audit, including proprietary information of the client itself. In addition to strict professional requirements, auditors are subject to stringent security and privacy provisions of the HIPAA when auditing health claims during an audit of a health and welfare plan. Noncompliance with professional standards and/or HIPAA could result in potentially severe consequences to the CPA, making an NDA unnecessary. The plan administrator should consider establishing reasonable procedural protections that provide practical alternatives to NDAs, including de-identifying and/or more carefully identifying the data to be exchanged in the course of an audit, and discussing these alternatives with service organizations.

Best practices for protection of PII and other sensitive information

Because any data that is stored is potentially vulnerable, it is important to develop policies and safeguards for protecting that data. Policies to consider include:

- Follow the "minimum necessary" and "business need" principles and only share the minimum amount of data (especially personal data) needed to accomplish a task.
- Reduce use of paper documents, as they cannot be encrypted.
- Retain only that information that is truly necessary for the business purpose. Collect less data and purge unnecessary PII from your records to reduce vulnerability.
- Shred purged paper documents with personal information in a secure disposal unit; do not use recycling or trash bins.
- Use caution in public spaces when handling or viewing personal information; be aware of your environment and use privacy screens on computers.
- Keep workspaces clear of documents containing personal information when not in use.
- Use secure methods to transmit personal information. For example, encrypt documents containing confidential information when emailing. Preferably, use an approved, secure collaboration site to transfer confidential data. Email generally should not be used to send personal information.
- De-identify data where possible. Mask or truncate government identifiers and health identifiers whenever possible.
- Control access to PII. Sensitive information should only be accessible by people who need it to do their jobs. This includes the information you share with your financial statement auditor. Check with your auditor to determine what PII is necessary for the audit.

The hiring of a service organization to assist in plan administration — such as bank trust departments, data processing service bureaus, insurance companies or other benefits administrators — is a fiduciary function. It is important that the service organizations you use to perform investment processing, recordkeeping and/or benefit payments, claims processing, and other services that require access to your plan's sensitive data have adequate protections in place to safeguard that information.

Plan administrators should perform adequate due diligence during the selection process and prior to hiring a service organization. In addition, as part of your fiduciary responsibilities, you are required to periodically monitor the service organization to ensure it is properly performing the agreed-upon services. The EBPAQC Plan Advisory, *Effective monitoring of outsourced plan recordkeeping and reporting functions* provides general information about selecting and monitoring service organizations. In addition, the following are suggested procedures that specifically address a service organization's handling of your plan's PII:

- Require the service organization to complete a detailed questionnaire to assess its services and ability to adequately protect PII.
- Define PII broadly to make sure it includes all sensitive information to which the service organization will have access.
- Obtain acknowledgement from the service organization that the services require the processing of the plan's PII, and it will:
  - Comply with the privacy laws that apply to that PII;
  - Keep PII confidential;
  - Provide information and support as the plan may require to comply with privacy laws;

  - Limit its use of the PII to the fulfillment of services described in the contract and for no other purpose; and
  - Permit the plan administrator to monitor the service organization's performance related to the protection of PII.
- Involve the plan's internal IT security personnel to evaluate the level of security offered by the service organization.
- Define a data security breach broadly to include suspected breaches and require that the service organization establish adequate procedures to prevent, detect, and remediate a breach.
- Require that the service organization notify the plan administrator of, investigate, and remediate a breach, and assist the plan with any required notices to affected individuals.
- Obtain and review a SOC 2® report each year related to the services provided and follow up on any items of concern. SOC 2® reports on an organization's controls that directly relate to the security, availability, processing integrity, confidentiality and privacy as a service organization.

In addition, the plan administrator should require the plan auditor, actuary, consultants, and others who provide professional services to the plan to:

- Ensure encryption when transferring electronic files, file passwords, etc.
- Establish physical safeguards over confidential information (for example, safeguarding of computers that contain confidential information, proper safeguarding of physical documents, etc.).
- De-identify claims information in audit documentation.
- Return or destroy written information, as required.
- Inform all engagement team members of their confidentiality obligations under the agreement with the client and their professional standards.

- Use SharePoint or a similar document management site to store client data.
- Restrict the printing of client materials. To the extent hard copies are used, prohibit removal of printed client materials from the client's site or the auditor's office.
- Only use audit firm-issued thumb drives that are encrypted.
- Direct any questions concerning IT security issues client.
- Share confidential information with as few team members as possible.

Plan accounting records and the financial statement audit

Audit scope and testing

Generally, ERISA requires employee benefit plans with 100 or more participants to have an audit by an independent qualified public accountant as part of their obligation to file an annual return/report (Form 5500 Series). To perform the audit of an employee benefit plan, the auditor will need access to a variety of plan and participant level records to perform testing and form conclusions on which to base the audit opinion. Therefore, it is important that the plan administrator maintain current and historical records that support the activity of the plan and the participants who participate in the plan. The following are common records and reports which the auditor might request when auditing the financial statements of an employee benefit plan:

- Plan document
- Adoption agreement
- Plan amendments
- IRS determination or opinion letter
- ESOP loan documents
- Copies of any correspondence with regulatory authorities
- Any investment contracts
- Trust agreements
- Service organization agreements
- Actuarial reports and written confirmation of selected information used in preparing the report
- Investment policy
- Information about internal controls related to plan operations and financial reporting
- A listing of all parties working with the plan

- Plan accounting records for the year being audited, including trust, custodian or insurance company statements and recordkeeper statements
- A detailed annual participant-level account summary
- A listing of all employees employed at any time during the year and dependents eligible for plan benefits (including name, unique identifier, demographic data necessary for determining eligibility, compensation and plan contributions)
- A listing of all benefit or claim payments made by the plan during the year being audited
- A schedule of contributions to the plan
- A listing of participant loans outstanding and new loans taken during the year
- A schedule of expenses paid and accrued by the plan
- Year-end payroll records
- Support for any plan mergers or transfers during the year
- Support for any prohibited transactions or litigation involving the plan

While this list might seem extensive, it is not all-inclusive and it represents only the initial information necessary to perform the audit. Once the initial information requested has been provided, the auditor will select samples of plan transactions and participants to test substantively. The information needed for the sample testing will depend on the type of plan, the nature of the transaction being tested, whether the plan has been audited previously, and the auditor's testing strategy. Because of these variables, it is not possible to provide a complete listing of what detailed information might be requested by the auditor; however, some examples of common requests might include:

- Demographic data support (such as date of birth, date of hire, or date of termination)
- Enrollment, deferral and investment election support
- Payroll information (in total and for selected participants for the year and for specific pay periods)
- Support for an individual's wage rate and hours worked
- A participant's account statement
- Distribution requests, including support for hardship payments, death certificates, or other items that support the type of distribution
- Support for an individual's vesting
- Support for the calculation of benefit payments (including payments to dependents eligible for plan benefits), including source documentation to support the inputs to the calculation
- Loan authorization forms
- Amortization schedules
- Rollover paperwork
- Expense invoices

Although the items noted above do not comprise a comprehensive list, they provide an indication of the volume of the data that is required for a plan auditor to perform an audit in accordance with relevant professional standards.

When a plan initially meets the requirements for an audit under ERISA, the auditor will need to audit the plan's opening balances. If your plan was previously audited by another firm, depending on the auditor's review of the information available from the prior auditor, the auditor might conclude additional testing of the plan's opening balances is necessary. Events such as plan mergers, plan spin-offs, a significant change in the number of plan participants, or a newly established plan also may result in an "initial audit" that requires auditing the plan's opening balances. Certain financial statement items may require that the auditor examine the accounting records and other information underlying the opening balances, which in an employee benefit plan, could span many years.

If the plan administrator is unable to provide the requested data, the auditor will have to consider whether there are alternative procedures that can be performed that allow the auditor to obtain sufficient evidence to opine on the financial statements. Alternative procedures may include confirmations with individual participants, obtaining source documentation from a third-party provider to the plan (for example, an actuary), or testing larger numbers of transactions rather than relying on sampling, all of which could be very costly. If alternative procedures cannot be performed, the auditor may be unable to obtain sufficient appropriate audit evidence in order to form an opinion on the financial statements.

The auditor's report and implications to the plan administrator

The significance of the plan records not made available to the auditor will dictate the type of report the auditor is able to issue. When the records are insufficient — even in circumstances beyond the control of the entity — it likely would result in a modification of the auditor's opinion (either a disclaimer of opinion or a qualified opinion).

A qualified opinion will be expressed when the auditor is unable to obtain sufficient appropriate audit evidence on which to base the opinion, but concludes that the possible effects on the financial statements of undetected misstatements, in any, could be material but not pervasive. The auditor will disclaim an opinion when he or she is unable to obtain sufficient appropriate audit evidence and concludes that the possible effects on the financial statements of undetected misstatements, if any, could be both material and pervasive.

When the auditor modifies the opinion on the financial statements due to an inability to obtain sufficient appropriate audit evidence, the auditor's report will include a "basis for modification" paragraph that states the reasons for that inability. In such cases:

- When the auditor expresses a qualified opinion, the auditor will state in the opinion paragraph that, in the auditor's opinion, except for the possible effects of the matter(s) described in the basis for qualified opinion paragraph, the financial statements are presented fairly, in all material respects, in accordance with the applicable financial reporting framework.

- When the auditor disclaims an opinion, the auditor will state in the opinion paragraph that because of the significance of the matter(s) described in the basis for disclaimer of opinion paragraph, the auditor has not been able to obtain sufficient appropriate audit evidence to provide a basis for an audit opinion, and accordingly, the auditor does not express an opinion on the financial statements.

It is important to understand that, generally, the DOL will reject Form 5500, *Annual Return/Report of Employee Benefit Plan* (Form 5500) filings that contain modified opinions (other than the limited-scope disclaimer that is permitted under the DOL Rules and Regulations for Reporting and Disclosure under ERISA). In addition to rejecting the Form 5500, the DOL has the right to assess penalties of up to $2,194 per day (indexed annually), without limit, on plan administrators for the deficient filing. In addition, fiduciaries who do not follow the basic standards of conduct may be personally liable to restore any losses to the plan.

As part of its fiduciary duties, the plan administrator is responsible for determining whether the plan meets the ERISA, DOL, and IRS record retention requirements, as well as the ERISA and DOL financial reporting requirements.

Inadequate plan records may also have negative consequences in defense of litigation, including significant legal costs and fees, and even unfavorable judgments. Many judgments have been entered against plan administrators for failure to produce documentation supporting the plan's participant benefit calculations.

Additional resources

EBPAQC plan sponsor resource center
The EBPAQC has compiled helpful tools and resources for plan sponsors, administrators and trustees.

DOL resources
U.S. Department of Labor Employee Benefits Security Administration Fiduciary Education Campaign website. The Fiduciary Education Campaign includes nationwide educational seminars and webcasts to help plan sponsors understand rules and meet their responsibilities to workers and retirees. The campaign also includes educational materials on topics such selecting an auditor.

Meeting Your Fiduciary Responsibilities
To meet their responsibilities as plan sponsors, employers need to understand some basic rules, specifically ERISA. ERISA sets standards of conduct for those who manage an employee benefit plan and its assets (called fiduciaries). This publication provides an overview of the basic fiduciary responsibilities applicable to retirement plans under the law.

IRS resources
IRS Revenue Procedure 98–25 provides taxpayers with comprehensive guidance on requirements for maintaining and providing IRS access to electronic tax records.

Notes

800.708.8775 | EBPAQC@aicpa.org | aicpa.org/EBPAQC