



A HEALTH PLAN TRUSTEE'S PLAYBOOK FOR EFFECTIVE VENDOR OVERSIGHT

by | Matthew Dubnansky

september/october 2026 **benefits magazine** ● 33

New transparency requirements and technological advances are raising expectations for fiduciary oversight of Taft-Hartley health plans, yet plans still struggle to obtain necessary data to monitor vendor performance—a key part of their fiduciary responsibility.

In addition, health plans have little prescriptive guidance from the Department of Labor (DOL) to govern fiduciary conduct.

To respond to these challenges, health plan trustees may want to consider implementing an integrated governance structure and formal vendor-monitoring program. This article discusses the fiduciary requirements for operating a health plan and provides a framework for effective oversight.

Background

The Employee Retirement Income Security Act of 1974 (ERISA) fiduciary standards apply equally to retirement and health plans; however, the DOL has not issued the same type of detailed guidance on fiduciary conduct for health plan fiduciaries that it has for retirement plans.^{1,2}

The benefit of this regulatory approach is that it provides group health plan fiduciaries with flexibility and the ability to adapt to changing market conditions. That can be particularly

helpful for Taft-Hartley plans, which are more complex to administer because they are governed through collective bargaining, often provide nonstandard benefit structures and are overseen by a joint labor-management board of trustees.

However, the downside is that it can create uncertainty, leaving room for interpretation and inconsistent application. As a result, similarly situated plans often adopt very different vendor oversight practices, ranging from comprehensive frameworks that include independently validated performance guarantees to relying on vendor self-reporting. Some might conduct operational reviews or react only when they receive a participant complaint. Because these approaches provide varying levels of assurance, they can expose plans to different degrees of fiduciary risk and increase the importance of professional judgment, advisor input and industry best practices.

Because plan fiduciaries, including boards of trustees that govern Taft-Hartley plans, may delegate certain responsibilities but retain fiduciary responsibility for prudent selection and monitoring of those delegates, effective oversight and monitoring of key third-party service providers is critical.

ERISA and the Duty to Monitor

ERISA requires fiduciaries to act solely in the interest of plan participants and beneficiaries, with the care, skill, prudence and diligence that a prudent person familiar with such matters would use and for the exclusive purpose of providing benefits and paying reasonable plan expenses.³

ERISA Section 405(c) permits fiduciaries to delegate certain responsibilities but that delegation does not eliminate fiduciary responsibility.⁴ DOL regulatory guidance and enforcement actions consistently state that fiduciaries must prudently select service providers, ensure that fees are reasonable and monitor provider performance on an ongoing basis.⁵ Courts have further interpreted the ERISA duty of prudence to require fiduciaries to actively monitor the service providers.⁶

This means that fiduciaries must have a process to evaluate vendor performance, verify compliance with plan terms and contractual obligations, and identify potential administrative or financial risks. Monitoring activities often include the following.

- Reviewing operational and financial reports
- Evaluating performance guarantees
- Conducting claims audits and compliance reviews
- Assessing cybersecurity controls
- Validating vendor-reported outcomes

takeaways

- Under the Employee Retirement Income Security Act (ERISA), Taft-Hartley health plan trustees may delegate certain plan functions to service providers, but trustees must monitor those vendors.
- New health plan transparency regulations may help fiduciaries more effectively monitor service providers and ensure that plan costs are reasonable; however, some plans still struggle to access necessary data.
- Health plan trustees should consider establishing an integrated governance structure that coordinates multiple monitoring processes to evaluate vendor performance, verify compliance with plan terms and contractual obligations, and identify potential administrative or financial risks.
- A risk-based methodology should be implemented to focus attention on service providers that present the greatest operational and financial risk to the plan.
- Proper vendor oversight begins with service provider contracts. Trustees must also address vendor issues appropriately and in a timely manner.

Oversight occurs when fiduciaries evaluate the results of these monitoring efforts, discuss findings in committee meetings, request explanations from service providers and direct corrective action when necessary.

Transparency Requirements and the Practical Challenges of Vendor Oversight

New disclosure requirements that attempt to address long-standing transparency concerns with third-party administrators (TPAs) and pharmacy benefit managers (PBMs) may help fiduciaries more effectively monitor service providers and ensure that plan costs are reasonable. The requirements are contained in the Transparency in Coverage rules and provisions of the Consolidated Appropriations Act (CAA) and recently proposed additional PBM transparency requirements.^{7, 8} These initiatives seek to improve price transparency, increase visibility into vendor compensation and expose PBM revenue streams.^{9, 10}

However, many boards of trustees still struggle to obtain the data they need to effectively evaluate vendor performance, since many plan contracts fail to compel access to data. Without consistent regulatory enforcement, this vendor resistance may persist unless fiduciaries proactively assert and document their oversight rights. In this environment, boards of trustees need clearly defined contractual rights, supported by structured governance practices and independent verification processes, to demonstrate prudent oversight of service providers.

Monitoring and Governance

Under ERISA, fiduciary conduct is assessed based on the specific situation

that the fiduciary faced at the time and whether a prudent person in a similar position would have acted in a similar manner.^{11, 12} As a result, oversight expectations vary based on factors such as plan size, benefit design, participant demographics, administrative complexity, information available to fiduciaries and prevailing industry practices for similarly situated plan fiduciaries.¹³

Lack of Coordination Hinders Effective Monitoring

Many Taft-Hartley plans align the level of monitoring with the relative risk presented by each key service provider. Plans may develop oversight activities over time through separate operational processes, such as financial reviews, performance reporting, compliance checklists and audit activities, without coordinating them within a unified governance framework. This lack of coordination could lead to fragmented information across different functions, which makes it more difficult for fiduciaries to evaluate vendor performance holistically and respond appropriately to emerging risks.

For example, many plans carve out administration of certain benefits, such as mental health and substance use disorder services, from the core medical benefits. In some cases, providers may submit the same claim for payment to more than one administrator, and because neither administrator knows what the other has paid, duplicate payments may go undetected. This may be because there is no process to evaluate how the combined administrative structure functions as a whole. If the plan does not have a coordinated way to identify or test risks that may come up when multiple service providers

are involved, they may not be detected through separate audits or vendor-specific reviews.

Similar issues can arise across medical and pharmacy benefits, as well as within network or repricing arrangements, where different vendors oversee related activities. Without a coordinated approach, these risks may not be identified through routine, vendor-specific reviews.

Creating an Integrated New Structure

Instead of building oversight practices for each separate vendor, boards of trustees should consider establishing a governance structure that coordinates multiple monitoring processes to evaluate vendor performance, verify compliance with plan terms and contractual obligations, and identify potential administrative or financial risks.

This structure can help ensure that these oversight activities are coordinated and aligned with the plan's overall risk-management framework. An effective structure should include the following elements.

- **Oversight supported by a clear governance model:** This model establishes how fiduciary oversight is organized, including the roles of the board of trustees, any delegated committees and the relationship between fiduciaries and service providers. A clear model helps ensure that fiduciaries exercise oversight intentionally and consistently, rather than developing informally over time or differing by vendor or function.
- **Clearly defined responsibilities:** Roles and responsibilities for monitoring, review, escalation and decision making should be

clearly articulated to avoid gaps or overlap across fiduciary and administrative functions. This helps ensure that key activities are assigned and completed, rather than assumed to fall within another party's scope.

- **Established reporting lines and review schedules:** Formalized reporting structures and review schedules help ensure that information flows to the appropriate fiduciaries on a timely basis and oversight activities occur with sufficient frequency. Regular reporting and documented reviews also support fiduciaries' ability to demonstrate a prudent, ongoing oversight process aligned with plan operations and risk exposure.
- **Governance that scales with the plan's complexity:** Oversight structure should reflect the plan's size, benefit design, number of service providers and administrative complexity. As plans introduce carve-outs, multiple vendors or more complex benefit arrangements, they may need to adapt their governance practices to address additional coordination risk and ensure that fiduciary oversight remains appropriate.

Prioritizing Oversight by Risk

Once the governance structure for oversight is established, boards of trustees can develop and annually apply a procedure to allocate monitoring resources appropriately and prioritize oversight activities to the vendors that create greatest risk exposure.

The service providers that pose the greatest operational and financial risks to plans typically administer benefits, manage costs and support plan operations. These vendors, including TPAs and PBMs, directly impact plan expenses, participant benefits and regulatory compliance, so they also represent areas of potential fiduciary risk.

The risk-based process evaluates the following:

- Each vendor's core function and how its services impact plan operations and participant benefits
- The financial and operational impact of vendor errors, noncompliance or underperformance

- The reasonableness, transparency and structure of vendor compensation and fees
- Vendor access to sensitive plan, financial or participant data
- The level of contract complexity and the ability to independently verify vendor performance.

Trustees should use risk tiering to determine the frequency and depth of oversight activities throughout the year. For example, in Taft-Hartley self-insured health plans, the TPA and PBM represent the areas of highest oversight risk because they directly influence the accuracy of claims processing, the application of plan benefits and the overall cost of health care services. Carve-out vendors that perform similar functions, such as third-party repricing or network pricing vendors, are another example of vendors that pose higher risks.

These vendors typically process the largest volume of financial transactions within the plan and operate under complex pricing and compensation arrangements, including rebate programs and administrative fee structures, that can have a significant impact on plan expenses and participant cost sharing. The use of automated claims adjudication systems and complex pricing algorithms in these arrangements can further increase operational complexity and oversight risk for plan fiduciaries.

Risk-based monitoring frameworks often prioritize oversight of TPAs and PBMs through structured reporting, performance monitoring and independent verification processes, such as claims audits, contract compliance reviews or other targeted evaluations.

Acting on Oversight and Monitoring Findings

Fiduciaries must take reasonable steps to address issues identified through monitoring in a timely manner. Failure to do so may constitute a breach of fiduciary duty.^{14, 15} Actions may include bringing concerns to vendor leadership, requesting corrective action plans, increasing oversight and reporting requirements, renegotiating contract terms and replacing vendors when necessary.

Documentation Is a Core Fiduciary Protection

Maintaining consistent documentation of the board's oversight activities helps demonstrate prudence, supports transparency in decision making and protects the board of trustees.

learn more

Education

**Self-Funded Health Plans: Plan Administration
E-Learning Course**

Visit www.ifebp.org/elearning for more details.

Boards of trustees should maintain records of the following.

- Annual risk-based assessment used to identify and prioritize areas for vendor oversight and review
- Vendor evaluations, including the scope of the review performed and any limitations encountered
- Reports and analyses reviewed by the board of trustees, along with the associated findings, observations and recommendations
- Board and committee discussions, deliberations and decisions, including any actions authorized or directed by the trustees
- Corrective actions taken by the vendor, including remedial plans and implementation steps, as well as the results of those actions
- Follow-up actions taken by the board of trustees to verify that identified issues were appropriately resolved and that corrective action measures were effective

Key Steps for Boards of Trustees

A coordinated, risk-based oversight process helps Taft-Hartley plan trustees fulfill their fiduciary duties to monitor service providers. Combined with regular reporting, performance monitoring and independent verification where appropriate, this process helps fiduciaries to timely identify and correct problems.

To translate these principles into practice, trustees may consider the following steps.

- **Establish a clear governance structure for oversight.** Trustees should define how oversight responsibilities are organized, including the role of the board, any delegated committees, and the process for escalating of issues for review and decision making.
- **Identify key third-party service providers and related administrative functions.** Trustees should maintain an inventory of service providers that directly impact plan costs, benefit administration, participant experience and compliance, such as TPAs, PBMs and other vendors supporting plan operations.
- **Assess related risk across vendors and functions and align oversight activities to the level of risk.** At least annually, trustees should evaluate which service providers and processes present the greatest potential operational, financial or compliance risk. Factors may include benefit complexity, reliance on judgment, data

Vendor Contracts Are the Foundation of Effective Oversight

Proper oversight begins with the service provider contract because it defines the plan's rights and the vendor's obligations. Contracts must align with the plan's governance and oversight framework. The plan attorney should work closely with the board of trustees and plan consultants who are responsible for oversight and monitoring activities to ensure that the contract includes the following key elements:



- Clear identification of core services and responsibilities, including the specific duties that the vendor is expected to perform and the standards by which those duties will be evaluated
- Audit rights that allow the board of trustees to verify performance, accuracy and compliance
- Data access provisions ensuring that the board of trustees can obtain the information necessary to evaluate performance, fees and outcomes
- Requirements that define the frequency, format and content of operational, financial and performance reports
- Performance guarantees and service-level standards tied to measurable outcomes as well as meaningful and enforceable remedies, including corrective action rights, fee adjustments or termination provisions
- Transparency obligations, including fee disclosures, compensation arrangements, subcontractors and pricing methodologies
- Cybersecurity and privacy requirements aligned with current regulatory expectations and the plan's risk profile.

Without these provisions, boards of trustees may find themselves responsible for monitoring vendor performance without having the contract rights necessary to do so effectively.

transparency, contractual limitations and the degree of coordination required across vendors. Higher risk areas may warrant more frequent reporting, targeted audits, cross-vendor reconciliation or independent verification, while lower risk functions may be monitored through routine reviews.

- **Coordinate reporting, review and follow-up within the governance framework.** Oversight results should

be reviewed through established reporting lines and at defined intervals, with clear responsibilities for addressing findings, tracking remediation and reassessing risk as circumstances change.

- **Reassess and refine the framework over time.** As plan design, service provider arrangements or regulatory expectations evolve, trustees should periodically revisit both the governance structure and the risk-based oversight approach to ensure that they remain aligned with the plan's current risk profile and operational complexity.

These steps support a prudent, process-driven approach to fiduciary oversight rather than prescribing a one-size-fits-all model. ERISA does not require fiduciaries to guarantee outcomes, but it does require them to engage in a prudent and well-reasoned process.

An integrated governance structure, combined with a risk-based oversight methodology, helps trustees move beyond fragmented or reactive monitoring and toward a coordinated approach that reflects the reality of modern plan administration. By doing so, trustees can better safeguard plan assets, protect participant benefits and demonstrate that they are fulfilling their fiduciary obligations in a thoughtful and defensible manner. 6

Endnotes

1. BDO, "Health Plan Held to Same ERISA Fiduciary Standards as Retirement Plans."

bio



Matthew Dubnansky, CPA, CGMA, is a partner based in the Columbia, Maryland office of Withum. He has more than 30 years of experience helping sponsors of self-insured health plans fulfill their fiduciary responsibilities through independent oversight of third-party administrators, pharmacy benefit managers and other service providers. Dubnansky regularly assists plan fiduciaries in identifying compliance risks, evaluating vendor performance and improving accountability across their health plan operations. He can be reached at mdubnansky@withum.com.

2. U.S. Department of Labor (DOL), Retirement Plans—compliance assistance and fiduciary guidance.
3. Employee Retirement Income Security Act (ERISA) 404(a)(1), 29 USC 1104(a)(1).
4. ERISA 405(c); 29 USC 1105(c).
5. U.S. Department of Labor, "Working With Service Providers."
6. *Tibble v. Edison International*, 575 U.S. 523 (2015).
7. Transparency in Coverage Final Rule, 45 CFR 147.212.
8. Consolidated Appropriations Act (CAA), 2021, Pub. L. No. 116 260, Div. BB, Title II, 202.
9. DOL *Field Assistance Bulletin* No. 2021 03.
10. Improving Transparency Into Pharmacy Benefit Manager Fee Disclosure, 91 Fed. Reg. 4348 (Jan. 30, 2026) (proposed rule).
11. *Tibble v. Edison International*, 575 U.S. 523 (2015).
12. ERISA 404(a)(1)(B), 29 USC 1104(a)(1)(B).
13. DOL, "Meeting Your Fiduciary Responsibilities."
14. ERISA 405(c); 29 USC 1105(c).
15. ERISA 405(a)(3), 29 USC 1105(a)(3).

benefits

MAGAZINE

Reproduced with permission from Benefits Magazine, Volume 63, No. 5, September/October 2026, pages 32-38, published by the International Foundation of Employee Benefit Plans (www.ifebp.org), Brookfield, Wis. All rights reserved. Statements or opinions expressed in this article are those of the author and do not necessarily represent the views or positions of the International Foundation, its officers, directors or staff. No further transmission or electronic distribution of this material is permitted.