TeamNash
A BOUTIQUE INSURANCE AGENCY

# HR Brief

**June 2026**

## Medicare Part D Changes Affecting Employer Plans for 2026 and 2027

The Inflation Reduction Act of 2022 (IRA) continues to reshape the Medicare Part D program through calendar years 2026 and 2027, with provisions designed to reduce beneficiaries' costs that may also affect employer-sponsored prescription drug coverage.

### Calendar Year 2026

- **Indexed annual out-of-pocket limit (OOP):** The annual OOP threshold is capped at $2,100 for 2026, reflecting an inflation adjustment to the $2,000 cap introduced in 2025.
- **Revised liability framework:** Part D includes revised liability to reflect negotiated prices taking effect for selected drugs in 2026.
- **Revised creditable coverage method:** For 2026 only, non-retiree drug subsidy (RDS) plans may use either the prior simplified method or a revised simplified method to determine whether their coverage is creditable.

### Calendar Year 2027

- **Coverage gap formally eliminated:** The Part D coverage gap or "donut hole" was eliminated in 2025 and is codified in the redesigned benefit.
- **Annual OOP limit:** The annual OOP cap remains in effect and continues to be indexed annually; once the limit is reached, enrollees have no additional cost sharing for covered drugs.
- **Prior creditable coverage method expires:** For 2027 and beyond, non-RDS plans can no longer use the prior simplified determination method; only the revised simplified method may be used.

### Employer Considerations

Employers that sponsor prescription drug coverage for Medicare-eligible individuals should become familiar with these developments, particularly as they relate to creditable coverage determinations. Employers and their benefit advisors may also consider monitoring prescription drug cost trends and reviewing existing cost-management strategies, as appropriate. Contact us today for more resources.

## 6 Tips to Avoid AI Scams

Artificial intelligence (AI) is transforming how organizations recruit, communicate and operate. Unfortunately, the same tools that are streamlining HR workflows are also fueling a new wave of sophisticated scams. Whether it's deepfakes of CEO voices or fake job applicants submitting AI-generated resumes, threat actors are exploiting AI to create more believable, personalized and scalable attacks. Consider these six tips to avoid AI scams:

1. **Recognize how AI is changing scam tactics.** AI enables increasingly convincing fakes, making it essential for HR teams to rely on process rather than instinct alone.
2. **Strengthen verification during hiring processes.** Building identity verification and scenario-based questions into every hiring stage can confirm authenticity in ways AI struggles to replicate.
3. **Validate communications claiming to be from leadership.** Always confirm unusual requests through a separate channel and question anything urgent that bypasses normal approval steps.
4. **Build processes that make scams harder to execute.** Multistep approvals and restricted data sharing reduce the risk that a single convincing message leads to a serious breach.
5. **Train regularly on AI threat awareness.** Frequent, targeted training (e.g., real scam examples and phishing simulations) is more effective than annual cybersecurity refreshers.
6. **Use technology as support, not the sole defense.** Combine AI-detection tools with human judgment and structured verification to ensure no single weakness becomes a failure point.

### Employer Takeaway

As AI-driven fraud becomes more sophisticated and widespread, HR teams are among the most targeted entry points for scammers. By staying informed, alert and proactive, HR can transform from a vulnerable doorway into a powerful first line of defense, helping the organization remain resilient in an evolving landscape of AI-enabled threats.