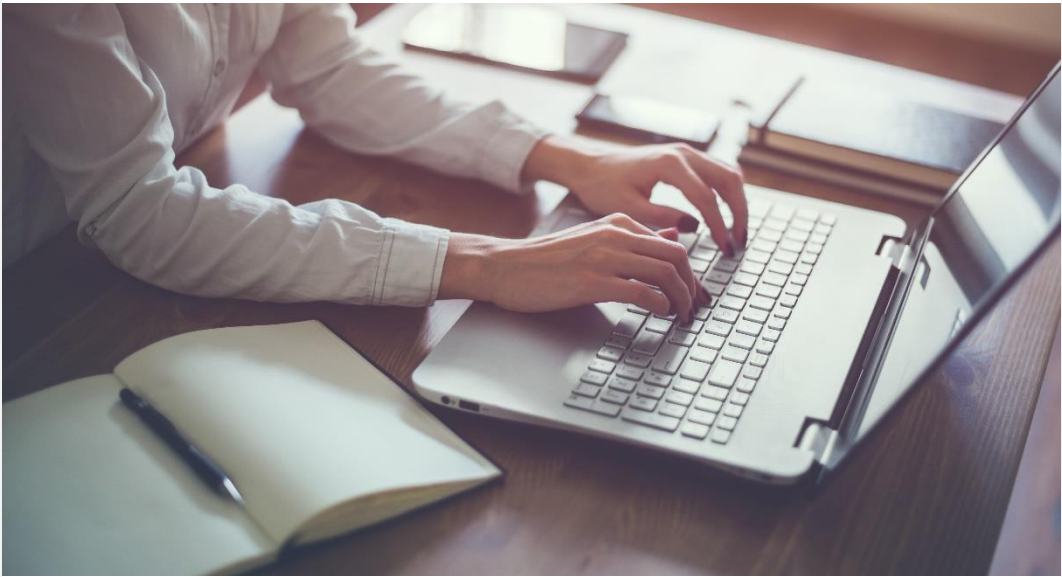


Deadline	Compliance Item	Applies To	Action Needed
July 31, 2025	PCORI Fee Payment - Pay Patient-Centered Outcomes Research Institute (PCORI) fee for self-insured health plans.	Self-insured health plans	File IRS Form 720 and pay fee
July 31, 2025 (for calendar year plans)	Form 5500 Filing - File annual Form 5500 for ERISA-covered plans with 100+ participants.	ERISA plan sponsors	File Form 5500 or request extension
September 15, 2025 (for calendar year plans)	PBGC - File annual Comprehensive Premium Filing and Premium Payment	ERISA plan sponsors	File PBGC Filing and pay premium

The key compliance deadlines noted above related to employer sponsored benefits is not exhaustive and other requirements may apply based on your entity's specific circumstances.



Rewards Policy Insider
2025-15



In this Issue:

1. [Compliance Reminder: Accelerated PBGC Premium Filing Deadline Approaches for the 2025 Plan Year](#)
2. [Supreme Court Will Not Review ERISA Preemption Case Involving Oklahoma PBM Law](#)
3. [HHS Reaches Settlement for HIPAA Violations After Cyberattack on Health Care Network](#)

Compliance Reminder: Accelerated PBGC Premium Filing Deadline Approaches for the 2025 Plan Year

For plan years beginning in 2025, a statutory change accelerates the premium filing deadline for pension plans to one month earlier than would otherwise be the case under the Pension Benefit Guaranty Corporation's ("PBGC") existing rules. For calendar year plans, the revised premium filing due date for this year is September 15, 2025 (instead of October 15).

Background

Under the PBGC's regulations that provide the rules for premium filing due dates, in most cases, the premium filing due date is the 15th day of the 10th calendar month that begins on or after the first day of that plan year (or October 15 for calendar year plans). This deadline is called the "Normal Premium Due Date." There are some exceptions for which a later due date applies, such as for a new plan that is adopted and effective less than 90 days before the Normal Premium Due Date.

Revised Premium Filing Deadline for Plan Years Beginning in 2025

A provision enacted as part of the Bipartisan Budget Act of 2015 ("BBA 2015") modifies the premium due date solely for plan years beginning in 2025. That is, for the 2025 plan year only, the premium filing due date is the 15th day of the 9th calendar month that begins on or after the first day of the plan year. In other words, for calendar year plans, the 2025 filing due date will be September 15, 2025 instead of October 15, 2025.

For plan years beginning in 2025, the revised due date supersedes both the Normal Premium Due Date and any special due date rules, such as the later deadline for new plans described above.

However, the BBA 2015's accelerated due date does not supersede the PBGC's disaster relief policy, which provides that when the Internal Revenue Service ("IRS") extends the Form 5500 due date for plans affected by a disaster, the PBGC automatically extends the premium filing due date for plans eligible for

the IRS's disaster relief. In addition, the accelerated due date does not affect the PBGC's rules extending due dates that fall on weekends or holidays.

Pension plan sponsors are advised that the following premium filing due dates apply for plan years beginning in 2025:

Date Plan Year Begins	Due Date
1/1/2025	9/15/2025
1/2/2025 - 2/1/2025	10/15/2025
2/2/2025 - 3/1/2025	11/17/2025*
3/2/2025 - 4/1/2025	12/15/2025
4/2/2025 - 5/1/2025	1/15/2026
5/2/2025 - 6/1/2025	2/17/2026*
6/2/2025 - 7/1/2025	3/16/2026*
7/2/2025 - 8/1/2025	4/15/2026
8/2/2025 - 9/1/2025	5/15/2026
9/2/2025 - 10/1/2025	6/15/2026
10/2/2025 - 11/1/2025	7/15/2026
11/2/2025 - 12/1/2025	8/17/2026
12/2/2025 - 12/31/2025	9/15/2026

*The 15th day of the ninth month beginning on or after the first day of the plan year falls on a weekend or federal holiday.

Supreme Court Will Not Review ERISA Preemption Case Involving Oklahoma PBM law

On June 30, the Supreme Court announced that it would not review the 10th Circuit Court of Appeals ruling that ERISA preempts certain key components of Oklahoma's law regulating pharmacy benefit managers (PBMs).

Background

It has been more than a year since the state of Oklahoma asked the Supreme Court to review the 10th Circuit's 2023 decision in *Mulready v. Pharmaceutical Care Management Association* (PCMA).

In *Mulready*, the 10th Circuit Court of Appeals ruled that ERISA preempts certain key elements of the Oklahoma law that regulate how pharmacy provider networks are designed and operated, including establishing geographic parameters for pharmacy networks, prohibiting incentives for participants to use certain in-network pharmacies – including mail-order pharmacies – over others, and imposing an “any willing provider rule” for pharmacy network participation. The 10th Circuit said that these types of network restrictions are state laws that mandate benefit structures, which ERISA explicitly prohibits.

In its decision, the 10th Circuit distinguished a prior Supreme Court ruling rejecting an ERISA preemption challenge to an Arkansas PBM law relating to

pharmacy reimbursements by PBMs. Unlike the Arkansas law, which the Supreme Court concluded was merely a form of cost regulation that is not preempted by ERISA, the provisions of the Oklahoma law at issue directly affect the ability of plans to structure their pharmacy networks and use cost-sharing to steer participants to preferred pharmacies, etc.

Supreme Court Decision to Not Review the 10th Circuit

Last October, the Supreme Court invited the U.S. Solicitor General to file a brief expressing the U.S.'s views on the case. In the brief it filed on May 27, 2025, the Solicitor General argued the 10th Circuit's decision was basically correct and that there was no need for Supreme Court review. The Solicitor General also argued that a future case might present a better opportunity for the Supreme Court to address ERISA preemption of state PBM laws. The Supreme Court apparently agreed with the Solicitor General's analysis, although it did not issue a written opinion providing a specific reason for its decision to not review the case.

Other states have passed laws similar to the ones at issue in Oklahoma, and it is possible that another circuit will reach a different conclusion than the 10th Circuit in a future case. If so, the Supreme Court may once again be asked to weigh in.

HHS Reaches Settlement for HIPAA Violations after Cyberattack on Health Care Network

The Department of Health and Human Services ("HHS") Office for Civil Rights ("OCR") continues to actively enforce the rules under the Health Insurance Portability and Accountability Act ("HIPAA"), as evidenced by a number of recent settlements, including one involving a phishing attack that targeted a health care network and resulted in the exposure of protected health information. This recent settlement serves as a reminder to employers that they should understand whether and how they and their group health plans are covered by HIPAA.

Background

Under HIPAA's Privacy Rule, "covered entities" – which includes health plans and most health care providers – and their business associates must protect the privacy of individuals' protected health information ("PHI") and follow certain limits on the use and disclosure of PHI. HIPAA's Security Rule requires covered entities and business associates to implement safeguards to protect electronic PHI, or "ePHI." HIPAA's Breach Notification Rule requires covered entities and business associates to notify HHS and any affected individuals in the event that their PHI has been compromised. These rules are enforced by the HHS OCR.

Settlement

In April, the HHS OCR [announced](#) a settlement with a California-based health care network involving potential violations of the Privacy, Security, and Breach Notification Rules. The violations stemmed from a “phishing” attack that exposed unsecured ePHI at the health care network. Phishing is a common type of cybersecurity attack which is designed to fool individuals into volunteering personal or financial information, often through fraudulent emails or other messages.

The phishing attack compromised the email accounts of 45 of the health care network’s employees, which resulted in the breach of nearly 190,000 individuals’ ePHI, including names, addresses, dates of birth, Social Security numbers, and lab results. Upon learning of this incident, the OCR conducted an investigation and found multiple potential violations of the HIPAA Rules, including: (1) failure to conduct an accurate and thorough analysis of the risks of ePHI held by the health care network; and (2) failure to notify affected individuals, the HHS Secretary, and the media of the breach within 60 days of discovery, as required by the Breach Notification Rule.

Under the terms of the settlement, the health care network agreed to implement a corrective action plan to protect ePHI (which the OCR will monitor) and pay \$600,000 to the OCR.

Big Picture

In a press release announcing the settlement, the OCR’s Acting Director warned that hacking is one of the most common types of large breaches reported to the office every year. With health care data being the target of increasingly sophisticated cyberattacks, and in order to avoid an OCR investigation, covered entities should periodically review and update their security procedures that cover PHI. It is clear that the OCR has been prioritizing investigations into phishing attacks targeting PHI ever since it settled its first-ever phishing attack investigation in December 2023.

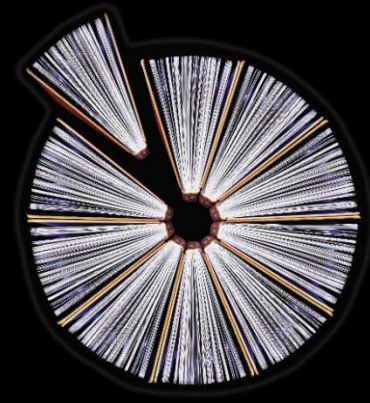
For plan sponsors, the HIPAA rules described above may apply in some circumstances – for example, employers with self-insured plans are not considered covered entities, but the plan itself would be considered a covered entity. Employers should ensure that they understand whether and how they and their group health plans are covered by HIPAA.

Visit the Archive

All previous issues of the Rewards Policy Insider are archived on Deloitte.com and can be accessed [here](#).

Don't forget to bookmark the page for quick and easy reference!

Upcoming editions will continue to be sent via email and will be added to the site on a regular basis.



Get in touch

Subscribe/Unsubscribe

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional adviser. Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms, and their related entities (collectively, the “Deloitte organization”). DTTL (also referred to as “Deloitte Global”) and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

Deloitte is a leading global provider of audit and assurance, consulting, financial advisory, risk advisory, tax and related services. Our global network of member firms and related entities in more than 150 countries and territories (collectively, the “Deloitte organization”) serves four out of five Fortune Global 500® companies. Learn how Deloitte’s approximately 330,000 people make an impact that matters at www.deloitte.com.

None of DTTL, its member firms, related entities, employees or agents shall be responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication. DTTL and each of its member firms, and their related entities, are legally separate and independent entities.

© 2025 Deloitte Consulting LLP

To no longer receive emails about this topic please send a return email to the sender with the word “Unsubscribe” in the subject line.