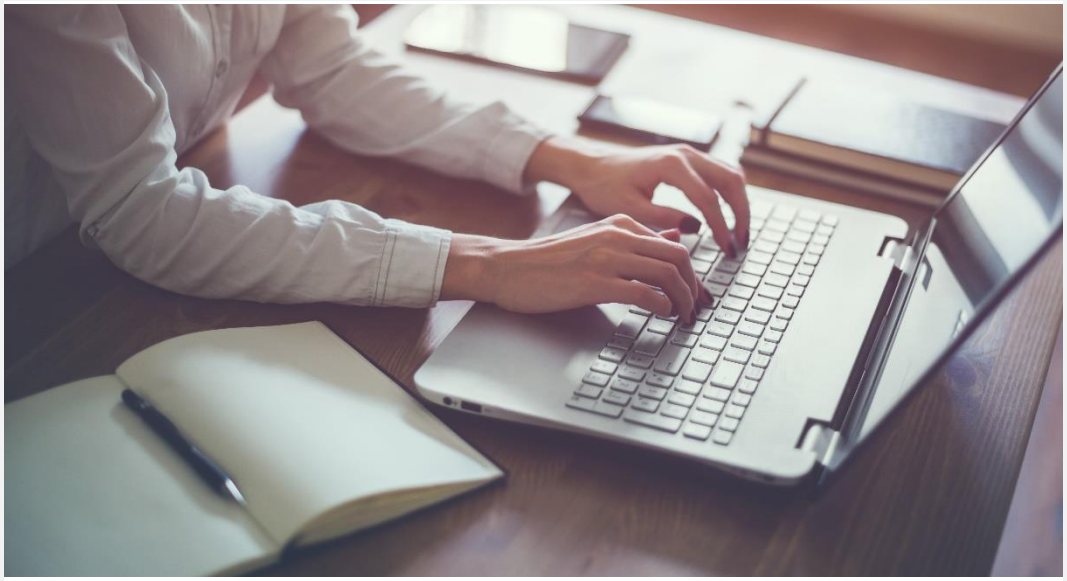
Deloitte.

United States | Human Capital | 24 January 2025

Rewards Policy Insider
2025-02



In this Issue:

HHS Proposes Updates to HIPAA Security Rule for First Time in Over a Decade

The Department of Health and Human Services ("HHS") proposed sweeping changes to the Health Insurance Portability and Accountability Act's ("HIPAA") Security Rule, which would require covered entities – including group health plans – to enhance their policies and procedures for protecting electronic personal health information ("ePHI").

The Security Rule

Under HIPAA's Security Rule, covered entities such as group health plans and most health care providers, as well as business associates of covered entities (collectively referred to as "regulated entities"), must implement safeguards designed to protect individuals' ePHI that is created, received, used, or maintained by the entity. The Security Rule, which was last updated in 2013, outlines the administrative, physical, and technical safeguards that regulated entities are required to implement. These technical safeguards must ensure the confidentiality of ePHI and protect against threats to ePHI.

Proposed Changes Would Ramp Up Required Cybersecurity Precautions

In a press release on the proposal, HHS highlighted the need to better protect the U.S. health care system from cyberattacks, which have become more frequent and more sophisticated. HHS also noted that the changes seek to address common deficiencies that the agency has observed when it conducts investigations into regulated entities.

Highlights of the proposal include:

- New Asset Inventory and Network Map. The proposed rule includes several new security standards that regulated entities would be required to implement, including a requirement that a regulated entity conduct and maintain a written inventory of its technology assets and a "network map" of its electronic information systems and all technology assets that may affect ePHI. The network map would show, for example, where the entity's technology assets are physically located on the worksite and where they are accessed through the cloud.
- Implementation Specification Terminology. The Security Rule currently contains two types of implementation specifications, called "required" and "addressable." Addressable implementation specifications permit a regulated entity to determine whether it would be reasonable and appropriate for the entity to implement the specification; if not, they must adopt an alternative measure. In order to clarify confusion about "addressable" being misinterpreted as "optional," the proposed rule would remove the "addressable" label altogether. Thus, regulated entities would be required to adopt all implementation specifications or adopt a reasonable alternative.
- Contingency/Incident Preparedness. The proposed rule would add a specific requirement that a regulated entity would need to establish a contingency plan for responding to an emergency – such as a natural disaster or system failure – that damages systems that contain ePHI.

One specific requirement would be that entities would need to establish written procedures to restore the loss of ePHI systems within 72 hours of the loss. Regulated entities would also be required to implement policies to address, document, and respond to suspected or known security incidents.

With the change in presidential administrations, it is not yet clear whether HHS under the Trump Administration will continue with this project or shift its focus to other priorities. If HHS does choose to move forward, the changes are proposed to be effective 60 days after an eventual final rule is published.

Supreme Court Hears Arguments in Significant ERISA Prohibited Transaction Case

ERISA took center stage at the Supreme Court on January 22nd, when the Court heard oral arguments in a case involving the question of what a plaintiff must allege in order to sustain a claim that a plan sponsor caused the plan to engage in a prohibited transaction in violation of ERISA. The outcome of the case could have significant impacts on the amount of litigation plans and service providers face for alleged prohibited transactions.

Background on Prohibited Transactions

ERISA section 406 provides that, unless an exemption applies, plan fiduciaries may not cause the plan to engage in certain "prohibited transactions," such as causing the plan to furnish goods or services between the plan and a service provider. Because plans frequently need to hire service providers, ERISA section 408 provides the exemption from that rule for the hiring of service providers as along as the services are necessary, the contract is reasonable, and reasonable compensation is paid for the services.

The Case before the Supreme Court

The Supreme Court is considering a case called *Cunningham v. Cornell University*, in which a group of plaintiffs sued a university, arguing that the university violated ERISA section 406 by hiring two service providers to provide recordkeeping services to its retirement plans. The U.S. Court of Appeals for the Second Circuit agreed with a lower court's dismissal of the claim and concluded that, for a plaintiff to advance a claim that the plan fiduciary engaged in a prohibited transaction by hiring a service provider, the plaintiff must show that the transaction was unnecessary or involved unreasonable compensation. The plaintiffs' argument was not sufficient to cross this threshold because they merely argued that the hiring of a service provider on its own is enough to state a claim for a prohibited transaction. The Second Circuit reasoned that it would not make sense for ERISA section 406 to prevent plans from hiring service providers outright because it would hinder their ability to hire providers that perform important recordkeeping and investment advising services.

The issue of the standard for a prohibited transaction was poised for Supreme Court review because several appeals courts are split on how they address the issue. In one camp, the Second Circuit and a handful of other circuit courts have concluded that a plaintiff must show that there was some wrongdoing in the transaction between the plan and service provider – for example, the compensation to the provider was too high or there is evidence that the plan fiduciary intended for the transaction to benefit the provider. In the other camp, a handful of circuit courts have established a very low bar for plaintiffs – i.e., to get past the preliminary motion to dismiss phase of a lawsuit, the plaintiff need only show that the plan hired a service provider in the first place.

Why is this Case Important?

The *Cunningham* case has been on the radar of many plan sponsors and service providers because the Supreme Court's decision could have a significant impact on the amount of litigation they face. If the Supreme Court adopts the low bar for plaintiffs to show that a prohibited transaction has occurred, class action plaintiffs will be able to advance their lawsuits to discovery, making litigation costlier and more burdensome for plans. A low bar could also mean that plans and service providers face a deluge of litigation from eager plaintiffs attempting to show a prohibited transaction has occurred, even if they do not have any evidence of wrongdoing on the part of the plan.

Plan sponsors and service providers following this case are hopeful that the Supreme Court will instead adopt the common-sense approach of the Second Circuit. In a positive sign, during the oral arguments, a few justices appeared to be very sympathetic to concerns over the potential for a wave of litigation if the Supreme Court adopts a low bar for prohibited transactions claims.

When Can We Expect a Decision?

We expect to see a decision from the Supreme Court sometime in the spring, although the Court could release a ruling at any point during its 2024-2025 term, which is expected to run through late June 2025.

IRS Releases Proposed Regulations on SECURE 2.0's Automatic Enrollment Requirements

Proposed regulations issued by the Internal Revenue Service ("IRS") would provide details on how the requirement under the SECURE 2.0 Act of 2022 ("SECURE 2.0") for 401(k) and 403(b) plans to automatically enroll their participants would work.

SECURE 2.0's Changes to Automatic Enrollment

Prior to the enactment of SECURE 2.0 in December 2022, retirement plans were permitted, but not required, to automatically enroll participants in the plan unless they opted out. In order to encourage employees to save for retirement, SECURE 2.0 now requires 401(k) and 403(b) plans to automatically enroll

participants at a minimum initial rate that can range from 3% to 10% and escalate that rate annually up to a minimum of 10% and a maximum of 15%. There are several types of plans that are exempt from this rule. For example, a 401(k) or 403(b) plan that was established before December 29, 2022 (the date SECURE 2.0 was enacted) are "grandfathered" and therefore not subject to these requirements.

The new requirements apply to plan years beginning in 2025.

Helpful Guidance Clarifies Automatic Enrollment Requirements

Because the statute left a number of unanswered questions on how exactly the new automatic enrollment rules would operate, on January 10, 2025, the Treasury Department and IRS released proposed regulations providing guidance on the provision. Generally, the regulations are proposed to apply to plan years beginning more than six months after the date that the future final regulations are issued.

Key takeaways from the proposal include:

- Grandfathered Plans. As noted above, plans that are "established" before December 29, 2022 are grandfathered and are not required to meet the automatic enrollment requirements. To address confusion about what "established" means in this context, the proposed regulations provide that a plan is established when it is adopted, not when it is effective. (This incorporates preliminary guidance on the automatic enrollment rules that the IRS published in late 2023 in Notice 2024-2.)
- Requirement Covers All Eligible Employees, Not Just Employees Eligible Starting in 2025. SECURE 2.0 was not clear on whether the automatic enrollment requirements would apply to all employees eligible to participate in the employer's plan, or whether they would apply only to employees who become eligible on or after the effective date for the rules, i.e., the 2025 plan year. The proposal clarifies that the automatic enrollment requirements apply to all eligible employees, without exception. Thus, any employee who did not already have an affirmative election in place to opt out of the plan would be automatically enrolled.

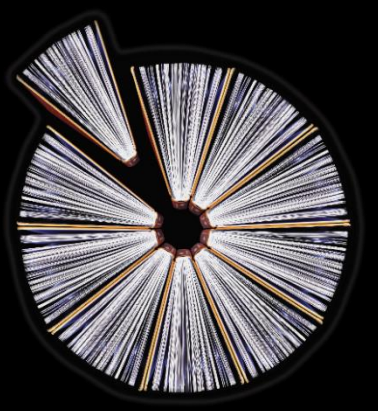
  The proposal also states that if an employer has not already complied with this requirement, then all employees who do not already have an affirmative election in place will have to be covered under the automatic enrollment requirements on the first day of the first plan year that the future final regulations apply to the plan.
- Guidance for MEPs and PEPs. As noted above, last year, the IRS provided preliminary guidance on the automatic enrollment rules in Notice 2024-2. In the Notice, the IRS said that if a single-employer plan that was grandfathered from the automatic enrollment rules merged into a multiple employer plan ("MEP") or pooled employer plan ("PEP") that was established after the enactment of SECURE 2.0, the single-employer plan would lose its grandfathered status. However, the proposed regulations would modify this unfavorable position so that such a plan would not lose its grandfathered status.
- Clarification of Exception for New Businesses. Under SECURE 2.0, the automatic enrollment requirements do not apply to new businesses that have been in existence for less than three years. The proposed regulations would clarify that when an employer surpasses the three-year mark, the employer's plan must meet the requirements beginning no later than the first plan year that begins on or after the third anniversary of the employer's existence.

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