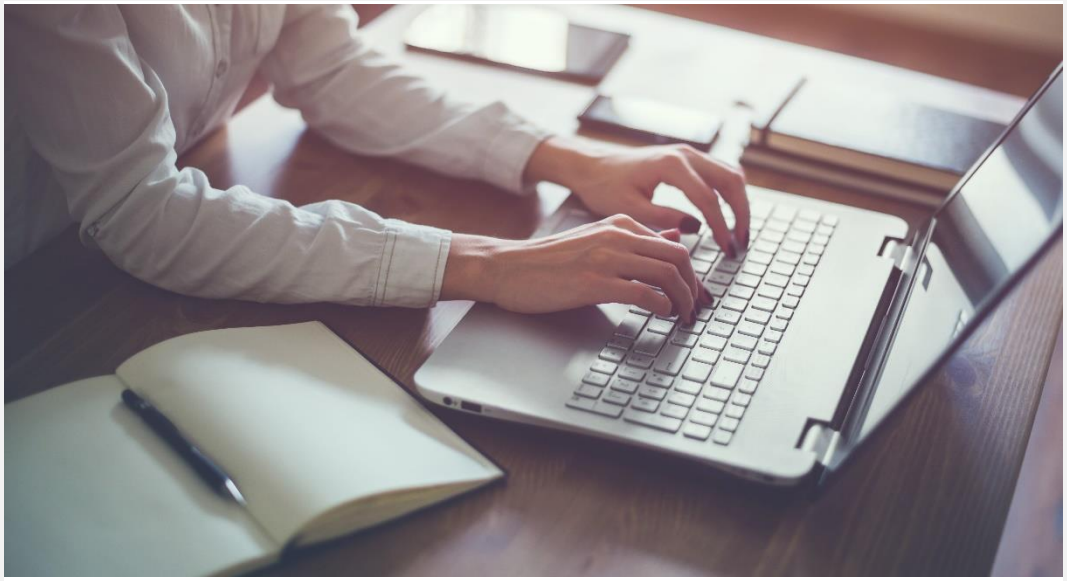
Deloitte.

United States | Human Capital | 4 October 2024

Rewards Policy Insider
2024-20



In this Issue:

DOL Updates Cybersecurity Guidance to Confirm Applicability to Health and Welfare Plans

The Department of Labor's ("DOL") Employee Benefits Security Administration ("EBSA") updated its 2021 cybersecurity guidance to confirm that the guidance applies to all employee benefit plans, including retirement, health, and welfare plans. The guidance provides tips for plan sponsors, recordkeepers, and participants to adhere to cybersecurity best practices.

Background

In April 2021, EBSA released guidance that provided cybersecurity tips and best practices for plan sponsors, fiduciaries, recordkeepers, and plan participants and beneficiaries. This guidance was prompted in part by DOL's increasing concerns surrounding the potential for cybersecurity incidents affecting plans and their participants, due to the amount of assets and the presence of sensitive personal information in plans. In the years since the guidance was released, EBSA said that it had heard from health and welfare plan service providers that the guidance applied only to retirement plans, not health and welfare plans. The 2021 guidance was not clear on this point.

Updated Guidance

In updated guidance released on September 6, 2024, EBSA addressed the uncertainty surrounding health and welfare plans by confirming in Compliance Assistance Release ("CAR") 2024-01 that the cybersecurity guidance issued by EBSA in April 2021 generally applies to *all* employee benefit plans, *including health and welfare plans*.

CAR 2024-01 also made relatively minor changes to the three documents that make up EBSA's cybersecurity guidance. As a refresher, key takeaways from the three pieces of guidance are highlighted below:

- Tips for Hiring a Service Provider. The Tips for Hiring a Service Provider are intended to help plan sponsors and fiduciaries prudently select a service provider with strong cybersecurity practices and monitor their activities, as required by ERISA. For example, the tips recommend that plan sponsors and fiduciaries ask about the service provider's information security standards and evaluate the service provider's track record in the industry, including information regarding any security incidents or litigation. The tips also recommend that plans ensure that the contract with the provider requires ongoing compliance with cybersecurity standards and warn plans to watch out for contract provisions that limit the provider's responsibility for IT security breaches.
- Cybersecurity Program Best Practices. The Cybersecurity Program Best Practices are intended to assist plan fiduciaries and recordkeepers in their responsibilities to manage cybersecurity risks. The best practices emphasize the importance of having a formal, well-documented cybersecurity program and conducting annual risks assessments.
- Online Security Tips. The Online Security Tips provide plan participants and beneficiaries with tips to reduce the risk of fraud and loss when

they check their account information online. For instance, the document provides tips on how to create strong passwords and encourages multi-factor authentication.

Implications for Employers

While EBSA's cybersecurity guidance is technically not binding – because CARs do not have the force of law – DOL is clearly interested in cybersecurity issues surrounding retirement and health and welfare plans. In the last few years, DOL's investigations and enforcement efforts have focused more and more on plan sponsors' and service providers' cybersecurity practices. To make sure they are prepared for any such audit from DOL, employers should review and strengthen their existing cybersecurity protocols or implement them if they do not already have such policies.

HHS Publishes Model Attestation for Uses and Disclosures of PHI Potentially Related to Reproductive Health Care

Pursuant to regulations issued earlier this year, the Department of Health and Human Services Office of Civil Rights has published a model attestation that HIPAA covered entities – including group health plans – and business associates can use to satisfy the new attestation requirement for protected health information (PHI) requests that are potentially related to reproductive health care.

Background and Summary

Responding to concerns that states with strict limits on abortions might seek information about individuals receiving reproductive health care from HIPAA covered entities (i.e., health plans, health care providers, and health care clearinghouses) for enforcement purposes, the Department of Health and Human Services issued updates to the HIPAA privacy rule to "support reproductive health care privacy." The final rule was published in the April 26, 2024 edition of the Federal Register, and is generally effective beginning on December 23, 2024.

In general, the final rule prohibits the use or disclosure of PHI for any of the following activities:

- To conduct a criminal, civil, or administrative investigation into or impose criminal, civil, or administrative liability on any person for the mere act of seeking, obtaining, providing, or facilitating reproductive health care, where such health care is lawful under the circumstances in which it is provided.
- The identification of any person for the purpose of conducting such investigation or imposing such liability.

If a HIPAA covered entity or business associate receives a request for PHI that is potentially related to reproductive health care, the covered entity or business associate generally must obtain an attestation that the request is not for any of the prohibited purposes identified above.

When an attestation is required, the model attestation can be used.

Effective Date

As noted, HIPAA covered entities and business associates generally must begin complying with the final rule relating to reproductive health care – including the attestation requirement – by December 23, 2024.

The final regulation also requires covered entities to update their HIPAA Notice of Privacy Practices. The compliance deadline for those updates is February 16, 2026.

Compliance Reminder: October 14th is Last Day for Group Health Plans to Provide Part D Creditable Coverage Notice

Group health plans that provide prescription drug benefits must notify all Medicare-eligible participants if the plan's prescription drug coverage is "creditable coverage." Plans must provide this notice on an annual basis before October 15th.

Background

Creditable Coverage Notice. Prior to the start of each year's Medicare Part D annual enrollment period on October 15th, group health plan sponsors that offer prescription drug coverage must provide a written notice of "creditable coverage" to all Medicare-eligible plan participants and their dependents, regardless of whether they are covered as active employees, COBRA beneficiaries, or retirees. This also includes those who are age 65 and older, as well as those who are Medicare-eligible due to disability or end-stage renal disease.

In general, prescription drug coverage is "creditable" when its actuarial value equals or exceeds the actuarial value of standard prescription drug coverage under Medicare Part D; in other words, it is expected to pay on average at least as much as the standard Medicare prescription drug coverage. In order to ensure that all individuals who should receive the creditable coverage notice actually receive it, some plans opt to send the notice to all participants.

In addition to the annual creditable coverage notice, the notice also must be provided in certain other circumstances, such as when a Medicare-eligible individual first joins the plan, whenever creditable coverage status changes, or upon the individual's request.

The notice is important because individuals who do not enroll in Medicare Part D when they first become eligible will be subject to a late enrollment penalty unless they maintain other creditable coverage.

Report to CMS. In addition to sending the creditable coverage notice to participants, group health plans are responsible for reporting their creditable coverage status to the Centers for Medicare & Medicaid Services (CMS) using the Online Disclosure to CMS Form. This annual disclosure should be completed no more than 60 days after the beginning of each plan year or within 30 days after any change in a plan's creditable coverage status. Additional information on these requirements, including links to official model notices of creditable coverage, are available on the CMS website.

Important Changes

In 2022, the Inflation Reduction Act enacted major changes to Medicare Part D, which go into effect on January 1, 2025. As a result of these changes, which generally redesign and enhance the Part D program, the actuarial value of coverage for Medicare Part D will increase. Thus, some plans that historically have had actuarial values equal to, or only slightly above, that of Medicare Part D may need to be enhanced in order to continue to be creditable coverage.

CMS has attempted to address the potential creditable coverage issues created by the IRA's changes to Medicare Part D for 2025. Specifically, CMS is allowing plans to continue using the creditable coverage simplified determination methodology, without modification, for 2025. However, the simplified method is not available to plan sponsors taking advantage of the Retiree Drug Subsidy program.

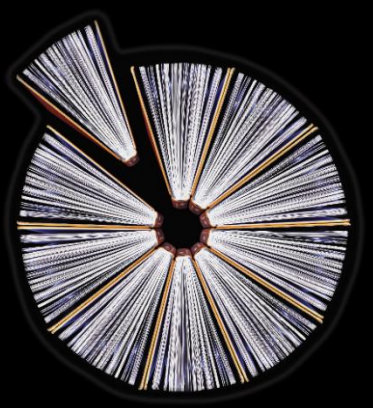
For 2026, CMS has indicated that it will re-evaluate the continued use of the existing simplified method or establish a revised one.

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