2022 Advisory Council on Employee Welfare and Pension Benefit Plans

Cybersecurity Issues Affecting Health Benefit Plans

Issue Chair: James Haubrock
Issue Vice-Chair: Shaun C. O'Brien
Drafting Team: Dave Gray, Marcelle Henry, Mercedes Ikard, Jeffrey Lewis, Tonya Manning

The 2022 Advisory Council will examine cybersecurity issues affecting health benefit plans. The examination will identify issues and vulnerabilities affecting these plans and faced by plan sponsors, fiduciaries, and service providers, as well as how those may differ by plan size. The Council will also examine existing relevant frameworks, approaches and initiatives tailored to health care and health plan cybersecurity concerns and the interaction between overlapping regulatory regimes for health plans.

Health-care-related privacy and cybersecurity challenges may also be implicated in the administration of disability or other welfare plans. The Council's examination will not generally address cybersecurity issues affecting welfare benefit plans other than health plans, such as long-term disability plans. The Council expects, however, that some of its findings and recommendations will be relevant to those plans.

The work of the Council is intended to assist the Department in determining whether there is a need for cybersecurity guidance, education or other initiatives related specifically to health information or health plans. It also will inform plan sponsors and fiduciaries about the vulnerabilities they face and resources available to address them. The Council hopes to hear from witnesses representing the federal government, the cybersecurity industry, those responsible for existing cybersecurity frameworks, the plan sponsor community, health insurers, plan service providers and others.

The 2016 Advisory Council studied cybersecurity considerations as they related to pension and welfare benefit plans. In doing so, the 2016 Council built on the work of the 2011 ERISA Advisory Council, which examined privacy and security issues affecting employee benefit plans. The 2016 Council recommended the Department make the Council's report available to plan sponsors, fiduciaries, and service providers to provide them with information on developing and maintaining a robust cyber risk management program for benefit plans. The Council also recommended the Department provide information to the employee benefit plan community to educate them on cybersecurity risks and potential approaches for managing these risks and drafted a sample document titled "Employee Benefit Plans: Considerations for Managing Cybersecurity Risks" as an illustration of the information the Department could provide. The 2016 Council did not address unique issues and vulnerabilities related to health plans.

In 2021, the Department issued three forms of sub-regulatory guidance on the issue of cybersecurity: (1) "Tips for Hiring a Service Provider" to help 401(k) and other pension plan sponsors and fiduciaries prudently select a service provider with strong cybersecurity practices and monitor their activities; (2) "Cybersecurity Program Best Practices" to assist plan fiduciaries and record-keepers in their responsibilities to manage cybersecurity risks; and (3) "Online Security Tips" to provide plan participants and beneficiaries who check their retirement accounts online basic rules to reduce the risk of fraud and loss.[1] The 2021 guidance did not address issues related specifically to health plans.

[1] https://www.dol.gov/agencies/ebsa/key-topics/retirement-benefits/cybersecurity (accessed June 13, 2022).