Armstrong Teasdale

August 3, 2021 • Publications • www.atllp.com

FOR YOUR BENEFIT NEWSLETTER, AUGUST 2021

HIV PREVENTION PILL (PREP) DESIGNATED AS PREVENTIVE SERVICE THAT MUST BE OFFERED WITHOUT COST-SHARING BY GROUP HEALTH PLANS

The Public Health Service Act (PHS Act) requires most employer-sponsored group health plans and health insurers to provide preventive care benefits without any cost-sharing for medical services that have an "A" or "B" rating from the United States Preventative Services Task Force (USPSTF). In 2019, the USPSTF recommended, with an "A" rating, that physicians offer PrEP, or pre-exposure prophylaxis, with antiretroviral therapy to those at risk for HIV infection because use of PrEP greatly reduces the likelihood of a high-risk individual contracting HIV.

However, earlier this year, an HIV advocacy group found that many plans and insurers were either requiring some form of copayment or not making it clear that no copayment is necessary for the treatment. Suggesting that PrEP may involve some out-of-pocket expenses likely discourages its use among those who are at a high risk of contracting HIV. Therefore, the Department of Labor, the Department of Health and Human Services and the Treasury issued guidance in the form of an FAQ, reiterating that covered plans and insurers must cover PrEP with antiretroviral therapy, and many services associated with encouraging consistent use of the treatment and monitoring patient health.

Ancillary services encompassed in the cost-sharing prohibition include periodic HIV testing, hepatitis B and C testing, creatinine testing and calculation of estimated creatinine clearance or glomerular filtration rate, pregnancy testing, and STI screenings and counseling. Additionally, covered plans and insurers may not require copays for adherence counseling, which is necessary to maximize the effectiveness of the treatment, nor may plans require copays for office visits with the primary purpose of delivery of these services when the services are not billed separately from the office visit or tracked as a separate encounter.

Issuers may use reasonable medical management techniques to restrict the frequency, method, treatment, or setting of the services *only* to the extent not specified in the USPSTF recommendation, which specifies that HIV testing should be performed before starting PrEP and every three months thereafter while on the regimen. However, the USPSTF recommendation does not require covered plans and insurers to cover the branded version of PrEP without cost-sharing. Plans may cover only the generic version without cost-sharing, unless

PEOPLE

Scott E. Hunt

SERVICES AND INDUSTRIES

Employee Benefits and Executive Compensation

the covered version is medically inappropriate for the individual. In that case, the insurer must have processes for waiving cost-sharing for the nonpreferred version that is expedient enough to allow an individual to begin PrEP on the same day that the individual receives a negative HIV test.

The FAQ provides that no enforcement action will be taken against covered plans and issuers who fail to provide required PrEP coverage for up to 60 days after the publication of the FAQ. Since the FAQ was issued on July 19, 2021, the 60-day grace-period ends on Sept. 17, 2021.

EEOC ISSUES GUIDANCE ON MANDATORY EMPLOYEE VACCINATION PROGRAMS AND VACCINE INCENTIVES

On May 28, 2021, the Equal Employment Opportunity Commission (EEOC) issued guidance for employers considering mandatory COVID-19 vaccinations for employees returning to work. The new guidance allows mandatory vaccinations; however, employers must weigh Americans with Disabilities Act (ADA) and Title VII considerations.

Reasonable Accommodations: Employers with mandatory vaccination programs will be required to provide reasonable accommodations as long as doing so would not create an undue hardship on the employer's business operations. The following circumstances will require a reasonable accommodation:

- Where employees have a disability or sincerely held religious belief preventing them from receiving a vaccination.
- Where a vaccination requirement would be applied in a manner resulting in disparate treatment for employees based on a protected classification (e.g., age, pregnancy, race, color or national origin). If there is a legitimate, nondiscriminatory reason for the requirement, employers may be protected.

Examples of reasonable accommodations employers can consider include:

- wearing facemasks;
- social distancing from other employees;
- regular COVID-19 testing;
- working remotely; and
- reassignment to a different location or job.

An employee does not need to specifically mention a "reasonable accommodation" or the ADA to qualify for an accommodation.

Employer Incentives: Employers may also provide incentives for vaccination, but such incentives may not be coercive as to pressure employees to provide protected medical information directly to the employer. However, if the employer does not arrange for or provide the vaccinations, this limit on the

provided incentive does not apply. Providing an incentive to encourage an employee to receive a vaccine may implicate other ERISA and tax issues. The details of the incentives should be reviewed for compliance with these rules, and an amendment to the employer's wellness or employee assistance plan may be prudent.

In order to avoid violations of other laws, employers may not offer an incentive to employees' family members to persuade them to receive a vaccination.

Confidentiality: Employers requiring vaccinations will need to keep all vaccine verification and other medical information confidential, regardless of where the employee receives a vaccine. Such information must be stored outside of the employee's personnel file.

MENTAL HEALTH PARITY ENFORCEMENT

Recently, with the passage of the Consolidated Appropriations Act, 2021 (CAA), the Departments of Labor, Treasury, and Health and Human Services (Departments) highlighted the required changes to mental health parity compliance documentation requirements for group health plans. Collectively, the agencies are beginning to examine group health plans' detailed comparative analyses, which plans are required to perform and document as part of their compliance with the federal mental health parity requirements. In recently issued FAQs, the Departments have clearly indicated that **general statements assuring compliance and/or conclusory references, without documentation to back those statements up, are not sufficient to demonstrate parity.** Instead, the Departments will be looking for detailed and well-reasoned explanations of the application of the nonquantitative treatment limitations (NQTLs) to mental health and substance use disorder (MH/SUD) benefits as compared to medical and surgical (MS) benefits in each of six benefit classifications.

The Departments confirmed that the Mental Health Self-Compliance Tool may serve as a guide to plans in performing comparative analyses. Generally, a detailed application of the Self-Compliance Tool will put plans on solid ground regarding compliance. The Self-Compliance Tool outlines four steps that plans must follow when analyzing NQTLs:

- In step one, the plan must identify the NQTLs in each classification.
- In step two, the plan must describe the factors that were considered in developing each NQTL.
- In step three, the plan must explain the sources it used to define each factor.
- Finally, in step four, the plan must demonstrate that all the factors, standards and processes identified in the preceding steps were comparable to and applied no more stringently to mental health

benefits than those that were applied to medical benefits.

Likewise, under the Departments' standards, sufficient analysis of compliance with the NQTL parity requirements must at a minimum contain the following elements:

- A clear description of the NQTLs and the plan's relevant terms and policies.
- Identification of NQTLs applicable to mental health and medical benefits in each classification (in- and out-of-network inpatient and outpatient benefits, emergency care and prescription drug benefits).
- The factors, evidentiary standards, or sources, strategies or processes considered in the design or application of the NQTL and in deciding to which MH/SUD and MS benefits the limitations will apply. The analysis must explain why any factors were given more weight and based on what evidence.
- If a plan defines any evidence in a quantitative manner, it must list precise definitions and sources to back up the evidence.
- If the plan's application of the NQTLs varied among MH/SUD and MS benefits, the plan must explain how it justifies the variations (with supporting factors and evidence).
- Where the application of an NQTL turns on the circumstances of a specific case, the plan must explain the nature and the timing of the decision and identify the decision-maker, as well as the decision-maker's qualifications.
- If the plan's analysis of the NQTL parity relies on an expert's opinions, the plan must document an assessment of the expert's qualifications and the extent to which the plan relied on the expert's recommendations.
- The analysis must include a reasoned discussion of the findings that the factors and standards outlined above are comparable among MH/SUD and MS benefits in each classification and not applied more stringently to MH/SUD benefits than to MS benefits. The written analysis must cite specific evidence considered and any results that lead to the conclusion that the plan is or is not in compliance with the NQTL parity.
- The analysis must list the date it was performed and the names, positions and titles of the persons that performed or participated in the analysis.

All analyses must be recent and not based on outdated information.

Plan sponsors and insurance issuers should be prepared to provide additional documentation to the Departments, including records of the NQTLs' development and application, claim processing guidelines, and details of any

internal testing or review done in determining the relative stringency of the NQTL applications, as well as evidence supporting the plan's conclusions.

The FAQs reminded plan sponsors that the Departments may identify noncompliance and give the offending plan 45 days to come into compliance and submit an updated comparative analysis report. If a plan fails to cure noncompliance, the Departments will notify plan enrollees of its conclusions. Furthermore, plan participants and their providers are entitled to receive comparative analyses reports regarding medical necessity. Plans subject to the Employee Retirement Income Security Act (ERISA) must also produce these analyses to claimants if any part of their claim is denied.

Although the Departments may request, and the plan must be ready to produce, comparative analyses of any and all NQTLs applied to MH/SUD benefits, the Departments have indicated that their initial focus is on four limitations:

- prior authorization requirements for in-network and out-of-network inpatient services;
- concurrent review for in-network and out-of-network inpatient and outpatient services;
- standards for provider admission to participate in a network, including reimbursement rates; and
- out-of-network reimbursement rates (plan methods for determining usual, customary, and reasonable charges).

For guidance or assistance with ensuring your group health plans are compliant with these mental health parity requirements, please contact one of our experienced attorneys, who can assist you.

NEW GUIDANCE PROVIDES BEST PRACTICES FOR ERISA FIDUCIARIES TO MITIGATE CYBERSECURITY RISKS

On April 14, 2021, the Department of Labor (DOL), through its Employee Benefits Security Administration (EBSA), issued guidance providing "best practices" for plan fiduciaries to ensure proper mitigation of cybersecurity risks. This marks the first time that EBSA has issued cybersecurity guidance as it relates to fiduciary duties under the Employee Retirement Income Security Act of 1974 (ERISA).

EBSA's guidance builds on existing regulations governing electronic records and disclosures to plan participants and beneficiaries, including provisions ensuring that electronic recordkeeping systems have reasonable controls, adequate records management practices, and that electronic disclosure systems include reasonable efforts to protect personal information of plan members.

The cybersecurity guidance addresses three areas involved in retirement plan administration. The links below each lead to a form from EBSA containing a

more in-depth look at each area:

- Tips for Hiring a Service Provider: This form provides guidance for **plan sponsors and fiduciaries** to assist with the prudent selection of a service provider with strong cybersecurity practices.
- Cybersecurity Program Best Practices: This form assists **plan fiduciaries and plan record-keepers** in managing their responsibilities to manage cybersecurity risks.
- Online Security Tips: This form provides information to **plan participants and beneficiaries** who check their retirement accounts online to reduce the risk of fraud and loss.

Prudently Selecting a Service Provider

Emphasizing the importance of ERISA's fiduciary requirements in selecting service providers, EBSA's guidance offers critical cybersecurity issues to consider when selecting service providers, including the following:

- Document the service provider's information security standards, practices and policies, and audit results, and compare them to the industry standards adopted by other related institutions. This also applies to third-party plan providers, even large, well-known organizations.
- Document the service provider's validation of its practice(s), methodologies and what levels of security standards, if any, it has met and implemented.
- Document the service provider's past security breaches, if any, what happened and how the service provider responded.
- Investigate whether the service provider has cyber liability insurance that covers damages and/or losses caused by cybersecurity and identity theft breaches, including misconduct by the service provider's own employees or contractors, or any other third-party breach(es).

Cybersecurity Best Practices

With regard to cybersecurity best practices, some of the EBSA's recommendations include:

- Maintain a formal, well-documented cybersecurity program.
- Conduct prudent annual risk assessments.
- Implement a reliable annual third-party audit of security controls.
- Follow strong access control procedures.
- Ensure that any assets or data stored in a cloud or managed by a third-party service provider are subject to appropriate security reviews and independent security assessments.

- Conduct periodic cybersecurity awareness training.
- Have an effective business resiliency program addressing business continuity, disaster recovery and incident response.
- Encrypt sensitive data, stored and in transit.

EBSA's guidance makes it clear that the DOL believes plan fiduciaries and third-party plan service providers should implement prudent safeguards that will adequately protect plan data. We would not be surprised to see the addition of these topics to DOL retirement plan audits.

If you have questions or concerns about the DOL's new cybersecurity best practices for retirement plans, please contact one of our authors, or your regular AT attorney.

Samra Cordic and Tess Butler also contributed to this edition of the For Your Benefit newsletter.