PILLAR
FINANCIAL GROUP

NEWSALERT
May 2025 | Volume 3 | Issue 5

Growing Threat

Cyber Criminals Target HSAs: Warn Your Employees

HEALTH SAVINGS accounts have become a prime target for cyber criminals, who are using advanced tactics to steal funds from them, putting your employees' medical expense savings at risk. The risk is even greater considering that employees can keep HSAs for life and many of them are building wealth in these accounts to save for future medical costs in their retirement years.

As the popularity and value of HSAs grows, employers are in a unique position to train their workers on how to best protect their accounts from cyberattacks that can drain their hard-earned medical expense savings.

Criminals see HSAs as ripe for plundering

HSAs have surged in popularity in recent years, with assets growing by 18% between mid-2023 and mid-2024 alone. There are an estimated 38 million HSA accounts in the U.S. with a combined $137 billion in funds, according to investment research firm Devenir.

Thanks to the portability of these accounts and the ability to invest them in investment funds — much like 401(k) plans — some HSAs hold large balances. That makes them especially appealing to cyber criminals.

While HSA providers have invested heavily in cyber security, threats continue to evolve because hackers aren't always breaching the providers directly. Sometimes, they gain access through third party vendors or by leveraging personal information leaked in unrelated breaches.

For example, HSA provider HealthEquity reported that attackers gained access to one of its business partner's accounts in 2024, potentially compromising the personal data of more than 4 million account holders.

Criminals may also send scam e-mails which direct account holders to bogus sites that steal their account username and password.

Once attackers have access to personal information, they may bypass security measures through phishing e-mails, social engineering tactics or brute-force password attacks.

In some cases, they exploit weak or reused passwords and intercept sensitive communications.

Employers can help

Given how deeply integrated HSAs are into employee benefits, employers can help by providing training that teaches their staff how to protect their HSA accounts and recognize phishing attempts or social engineering scams.

Cyber-security education doesn't have to be complex. Even short, focused sessions on topics like password hygiene, spotting suspicious e-mails and using multi-factor authentication can make a significant difference.

See 'Train' on page 2

PILLAR
FINANCIAL GROUP

7110 N Fresno St., Suite 120
Fresno, CA 93720

Phone: 559.436.6441
info@pillarcentral.com
pillarcentral.com

PILLAR
FINANCIAL GROUP

Boosting Awareness

Most Employees Unsure about How Health Insurance Works

ONE OF the biggest challenges for employers who offer their workers health insurance benefits is that the majority of U.S. workers are really in the dark about how insurance works, according to a new survey.

Despite employers' best efforts to provide as much education as possible to their workers before and during open enrollment, it seems the finer points are not sinking in, according to United Healthcare's "Consumer Sentiment Survey."

Survey Finds Low Understanding

- A mere 7% of those surveyed had a full understanding of all four basic insurance concepts: plan premium, deductible, coinsurance and out-of-pocket maximum.
- More than 60% of respondents could define plan premium and deductible.
- 36% could define out-of-pocket maximum.
- 32% could define coinsurance.

These deficiencies result in more people spending more on coverage than they may actually need to.

Another study, by the Kaiser Family Foundation, found that not having correct information can lead to dissatisfaction when employees discover they've signed up for a plan that doesn't meet their needs.

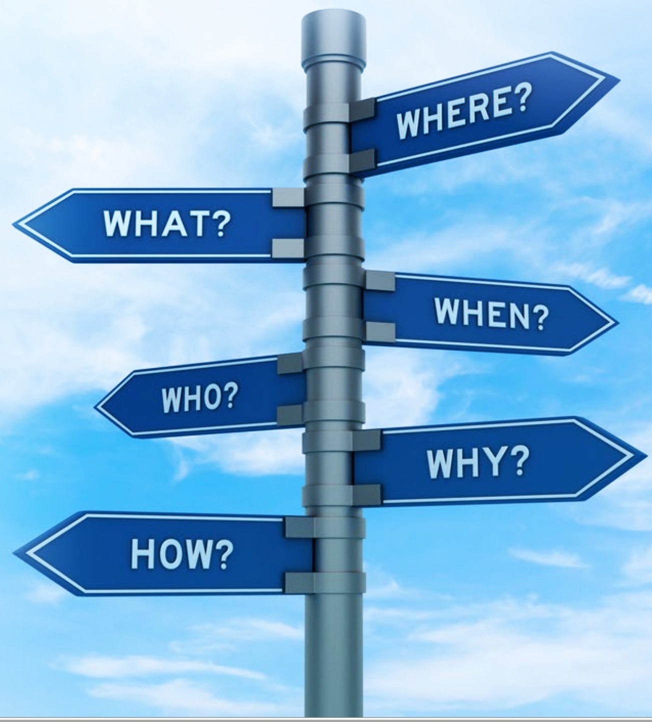
The Kaiser survey revealed that employees are most confused when it comes to understanding these factors:

- How to calculate out-of-pocket costs once claims are processed.
- The concept of providers who are in network versus out of network at an in-network hospital.
- Understanding deductibles and out-of-pocket annual limits for their plans.
- What a health insurance formulary is (concerning prescription coverage amounts).

So, as open enrollment nears, you may want to consider focusing on the foregoing areas to better educate your workers. Also, it's recommended that you approach the education process with a multi-pronged approach employing technology, meetings and the optional one-on-one time to cater to people's different learning styles.

It's important for your employee morale and their pocketbooks that they understand what their choices are and what they're buying. The more light you can shine on the process and the more stress you can reduce, the better off your employees will be.

This is especially true in light of one other finding in the United Healthcare study: One-fourth of respondents said they would rather file their annual income taxes than select a health plan. ❖



Continued from page 1

Train Your Staff on How to Protect Their HSAs

Here are some steps every HSA holder can take:

- **Monitor account alerts and e-mails:** Always check for e-mails or notifications about changes to your account, like updated contact info or security settings. If something looks unfamiliar, report it to your HSA provider immediately.
- **Review account transactions regularly:** Just like with a bank or credit card statement, it's important to review your HSA transactions to ensure all activity is legitimate. Most providers allow users to freeze their benefits card if they suspect fraud.
- **Use strong, unique passwords:** Never reuse passwords across accounts, and consider using a password manager to create and store complex, randomized passwords. The longer and more unique the password, the better.
- **Enable multi-factor authentication:** For added security, many providers are expanding user authentication options like sending verification codes via text or e-mail, or adding biometric verification. ❖

Weight-Loss Drugs

The GLP-1 Dilemma: How Employers Can Take Control

MANY EMPLOYERS are facing challenges in incorporating high-cost GLP-1 medications, such as Mounjaro, Ozempic, Rybelsus, Trulicity and Wegovy, into their group health plans, as they must balance the cost of the group health plan against the interests of participants and beneficiaries.

While most health plans will cover these drugs for individuals who have diabetes and obesity, employers have been loath to cover them for employees who just want to lose weight due to the immense costs — around $1,000 a month.

Despite that, employer spending on GLP-1s solely for obesity jumped nearly 300% between 2021 and 2023. And with demand continuing to increase, many employers are looking for ways to accommodate coverage for weight loss without breaking the bank. Here's what some of them are doing:

Taking a holistic approach

One of the major drawbacks when taking a GLP-1 to lose weight is that once a patient stops taking injections, they often gain the weight back and any improvements in their blood pressure, blood sugar levels and cholesterol may disappear.

This is why more employers who are covering GLP-1s for weight loss are also requiring the employees to take part in weight-management or lifestyle programs, like a dedicated exercise regimen and adopting a healthy and sensible diet.

With this approach, patients have a better chance of maintaining their weight loss if they stop taking the drug.

Set conditions

Experts recommend setting certain conditions to qualify for a GLP-1 prescription solely for weight loss. This may include requiring that they have a body mass index of 33 or higher (anything over 30 is considered obese) along with one comorbidity like:

- High blood pressure,
- Chronic obstructive pulmonary disease,
- Diabetes,
- Heart disease, or
- Respiratory disease.

Setting a lifetime limit

Some employers and health plans cap the amount that they spend on a GLP-1 for patients who want to lose weight. Some set an expense limit like $10,000 or $20,000, while others have a time limit, such as two years.

Higher copays and deductibles

Another strategy is setting a higher copay for GLP-1s. Also, since these drugs are not included on the ACA preventive service list, plans may introduce a deductible for this category of prescription drugs, provided that GLP-1 coverage is not required for preventive diabetes services.

Have an alternate solution

Another option is to cover bariatric surgery, which yields better results. It typically costs between $10,000 to $15,000 — about the same as one year of most GLP-1 prescriptions. Most people who undergo this type of surgery have a much higher success rate of keeping weight off.

After this surgery, many patients steadily lose weight during the first two years after the surgery, after which the typical patient regains less than 25% of their weight. Most people who stop taking GLP-1s cannot expect similar success in keeping their lost weight off.

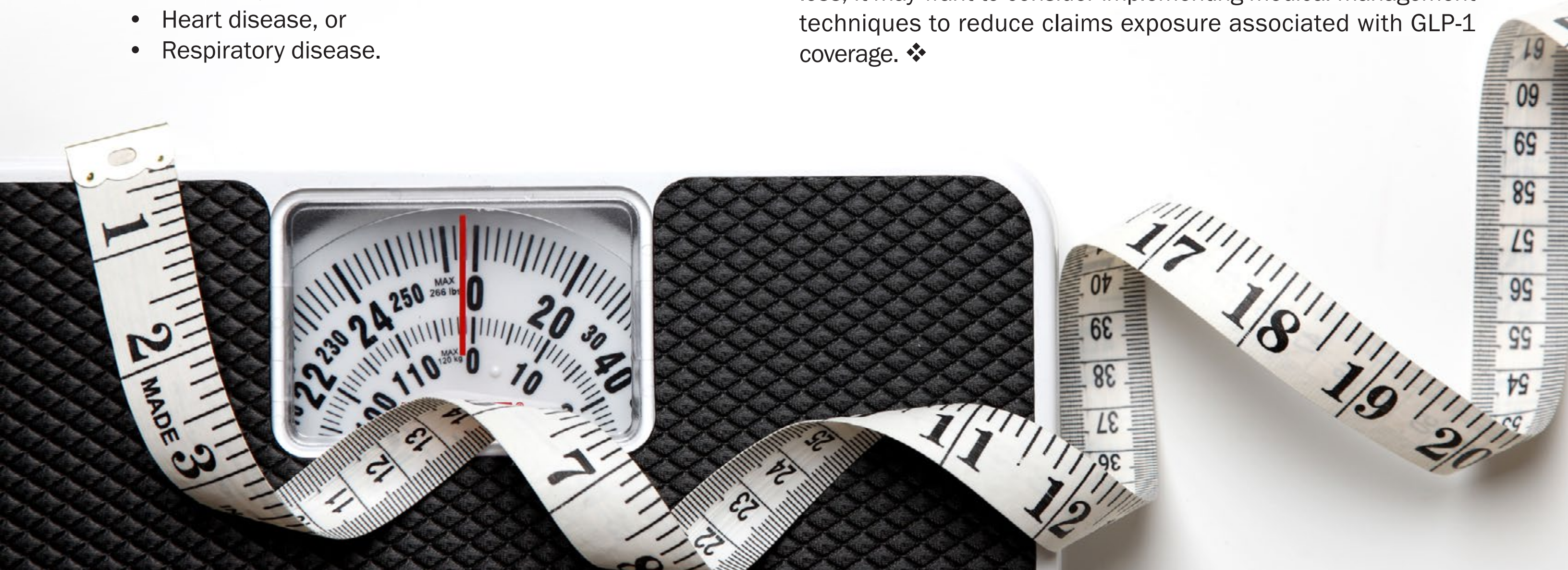
Step therapy

Step therapy is a medical management technique that requires the use of generally less expensive treatments before allowing coverage of higher-risk, higher-cost treatment options.

The takeaway

Currently, self-funded and fully insured group health plans are not required to cover GLP-1s for any purpose. However, because GLP-1s are a common form of treatment for diabetes, it may be difficult to exclude all GLP-1 coverage.

If a plan sponsor intends to provide GLP-1 coverage for weight loss, it may want to consider implementing medical management techniques to reduce claims exposure associated with GLP-1 coverage. ❖



EEOC's New DEI Guidance Explained

THE EQUAL Employment Opportunity Commission, together with the Department of Justice, recently issued new guidance that significantly reshapes the legal landscape for workplace diversity, equity and inclusion programs.

This comes on the heels of a series of executive orders issued by President Trump that direct federal agencies to eliminate what the administration characterizes as "illegal DEI" practices.

On March 19, the EEOC and DOJ issued two technical assistance documents meant to clarify how Title VII of the Civil Rights Act applies to DEI programs. While the documents reflect long-standing principles of anti-discrimination law, they also take a narrower view of what DEI initiatives are legally permissible.

For employers — especially those with formal DEI programs — this development creates new legal exposure, murky compliance territory and growing uncertainty around what is now permissible.

While the guidance outlines several potentially unlawful DEI practices, this ambiguity puts employers in a difficult position because the line between compliant and noncompliant practices is often hard to draw.

Below is a practical breakdown of what's changed, what remains unclear and what senior leadership should consider doing now.

The guidance

The agency said DEI policies, programs or practices may be unlawful under Title VII if they involve "an employment action motivated — in whole or in part — by an employee's race, sex, or another protected characteristic."

The guidance also emphasizes that protections apply equally to majority and minority groups.

Main Changes

Based on various legal interpretations of the guidance, the following are some of the most significant changes:

No exceptions for diversity goals – The guidance states there is no "diversity interest" exception under Title VII.

Affinity and resource groups must be open to all – Employers cannot restrict participation in affinity groups based on race, sex or similar traits.

No segregated programs – Holding training or other programs that separate participants by race, gender or other protected categories is likely unlawful.

No quotas – The EEOC reiterated that hiring or promotion quotas, or any form of "balancing" the workforce based on demographic traits, is discriminatory.

There is no "reverse discrimination" – Title VII protects all employees, regardless of group status. It does not require a higher burden of proof for claims from majority-group employees.

Steps employers can take

Given the legal uncertainty, the law firm Fisher Phillips recommends that companies consider the following actions:

- Engage legal counsel to review DEI-related policies, training materials and communications. Focus on areas such as hiring, promotion, compensation, training, mentorship, internships and affinity group policies.
- Shift from targeted DEI initiatives based on protected characteristics to programs that promote skill-building, access and inclusion for all employees. Emphasize transparent, merit-based advancement and development opportunities.
- Ensure programs emphasize workplace culture, professional development and merit-based access to opportunities.
- Update your training to reflect the latest EEOC guidance. Make sure that decision makers understand that DEI efforts cannot involve preferences or separate treatment based on protected traits.

Bottom line

The new guidance is a major shift in how the EEOC will approach regulating workplace discrimination. For employers, this means a narrower path for legally compliant programs and greater exposure to discrimination claims from any employee group.

If you have a workplace DEI program, it's imperative that you revisit it and adjust it accordingly. ❖