NEWSALERT
WEVODAU
Insurance & Benefit Strategies
a division of GUNN MOWERY

October 2024

ACA Compliance

Group Health Plan Affordability Level Up Sharply

THE IRS has significantly increased the group health plan affordability threshold — which is used to determine if an employer's lowest-premium health plan complies with the Affordable Care Act rules — for plan years starting in 2025.

The threshold for 2025 has been set at 9.02% of an employee's household income, up from 8.39% this year. The higher threshold will give employers a little more wiggling room when setting their employees' premium cost-sharing level for their lowest-cost plans in 2024.

Under the ACA, "applicable large employers" — those with 50 or more full-time or full-time equivalent employees (FTEs) — are required to offer at least one health plan that is considered "affordable" based on a percentage of the lowest-paid employee's household income. If an employer's plan fails this test, the employer may face penalties.

Safe harbors

The new threshold will apply to all health plans whenever they incept in 2025. The affordability test applies only to the portion of premiums for self-only coverage. Employers can use on one or more safe harbors when determining if coverage is affordable:

- The employee's W-2 wages, as reported in Box 1 (at the start of 2022).
- The employee's rate of pay, which is the hourly wage rate multiplied by 130 hours per month (at the start of 2022).
- The federal poverty level.

Example 1

The lowest-paid worker at Company A earns $27,000 per year. To meet the 2025 affordability requirement, they would have to pay no more than $2,435.40 a year in premium (or $202 a month).

Example 2

Company B has a large low-wage workforce and may utilize the current federal poverty level ($15,060) safe harbor and offer at least one health plan option that costs FTEs no more than $113.20 per month.

If an employee's coverage is not affordable under at least one of the safe harbors and at least one FTE receives a premium tax credit for coverage they purchase on an ACA exchange, the employer may have to pay a employer shared responsibility payment.

This penalty for 2025 will be $4,350 per employee that receives a premium subsidy on an exchange, down from $4,460 this year.

The takeaway

As 2025 nears, you should review your health plan costs and premium-sharing to ensure that your lowest-cost plan complies with the affordability requirement.

Please feel free to call your Wevodau agent if you have any questions. ❖

WEVODAU
Insurance & Benefit Strategies
a division of GUNN MOWERY

Wevodau Insurance & Benefit Strategies

600 N. Front Street,
Wormleysburg, PA 17043

Phone: 717-761-0393
Email: emily@wevins.com
website: www.wevins.com

‘Nuclear’ Jury Verdicts Are Straining U.S. Businesses

THE SIZE of jury awards has been exploding in the last few years, and they are often exceeding the limits that businesses have on their liability policies.

These excessively large awards are known as “nuclear” verdicts, which are defined as those with damages of $10 million or more. In 2023, such verdicts totaled $14.5 billion, according to one analysis.

In 2020, half of them were greater than $21 million; that number jumped to $44 million last year. There were 89 nuclear verdicts in 2023, and 27 of them were for more than $100 million.

This is happening at the same time that corporations in general are purchasing smaller amounts of liability insurance, according to a report by major insurer Chubb.

The median limits of insurance purchased have shrunk over the last 10 years. They are 44% less today in the construction industry than they were in 2014, 31% less in health care and 28% lower in consumer products.

This has created a large and growing gap between the amounts of insurance corporations are buying to protect themselves and the jury verdicts they may face. When a jury award surpasses a policy’s limit, the insured has to cover the rest out of pocket.

Recent nuclear verdicts:

- In Georgia, a truck veered into oncoming traffic, causing a driver to swerve out of its way and strike a man exiting his truck in the emergency lane. A jury ordered the trucking company to pay $47 million to the man’s family.
- In Seattle, a jury awarded a former ultramarathon runner $13.1 million in damages for a crippling injury she suffered when she fell on a sidewalk.

Investors financing lawsuits

Analysts have pointed to several reasons for the increase in these verdicts. People today are pessimistic, they have lost trust in corporations, they have become desensitized to large numbers, and they are more pro-plaintiff, according to these explanations.

However, another major factor is how these suits are financed. Lawsuits have become an investment vehicle for hedge funds and other large investors through a concept known as “third party litigation funding.”

In a TPLF arrangement, investors fund plaintiffs or law firms for the costs of these lawsuits. The benefit they receive is contingent on the suit’s outcome. If the plaintiff wins, the investors receive a share of the awarded damages. If the plaintiff loses, they get nothing.

Given that they invested $15.2 billion in TPLF arrangements in the U.S. in 2023, they appear to be optimistic about their chances.

TPLF provides financial incentives to file frivolous lawsuits because defendants may choose to settle cases rather than go to trial. The investors also get a say in whether or when to settle a suit. They may push for a trial in the hope of a nuclear verdict.

Because TPLF increases liability insurance premiums, out-of-pocket damage payments, or both, it increases corporations’ costs.

The takeaway

Liability insurance rates have been rising as a result of these nuclear verdicts, which you have probably noticed on your last premium bill. However, the worst thing you can do is reduce your limits, particularly in light of increasing jury awards.

And it’s not just nuclear awards that have become a problem. Awards are increasing for small cases, as well. ❖

Identify Workers' Needs, Consider Costs to Plan Benefits

IT'S ALMOST time for group open enrollment for policies that start Jan. 1, 2025 and you need to drive engagement so that your staff can make informed decisions about their health insurance options.

We want to help you help your employees understand all of their options so that they can purchase a plan that is appropriate for their situation. So here is our advice for open enrollment:

Listen to your workforce

Before you make any decisions, you should listen to your employees and better understand their needs and preferences.

With answers and feedback in hand you can create a benefits package which is more appealing to them, which in turn gives you a competitive edge when attracting and retaining workers.

Engage employees and solicit feedback through quarterly employee-benefits round table meetings. Invite employees from different age groups and departments to participate in these meetings to ensure you have a good cross-section of your staff represented.

Give advance notice

You can start this month with simple reminders for them to start thinking about open enrollment and evaluate their current health plans. Send out memos and place posters in high-traffic areas at your worksite.

If you start with this in September or October, they can have time to assess their options, particularly if anything has changed in their lives like marital status, new children or health issues.

Costs are paramount

You can work with us to settle on plan arrangements that will be within your and your employees' budgets (in their case, the plans also have to be deemed affordable under the Affordable Care Act).

Employees have a right to understand the costs, so let them know how to access the free transparency tools provided online by most medical carriers. Provide employees with a breakdown of medical and pharmaceutical cost increases to avoid sticker shock.

Get an early start

If your plan year starts Jan. 1, you should hold open enrollment meetings and dispense plan materials in October or November.

Avoid holding meetings in December. It's too busy and the ramping up period is too short..

Communicate effectively

Your task is to get employees out of cruise control and truly assess all of their options.

This is especially true if you are making changes to cost-sharing, introducing new plans, introducing a wellness plan or health savings accounts or flexible spending accounts.

You should use a variety of different media to communicate with your workforce.

Use video, virtual and live meetings, e-mail communications and print materials to get through to your employees. While the attentive ones may think it's overkill, using different forms of communication ensures that you reach the widest number of staff.

Get spouses involved

If you also offer insurance to spouses, you should communicate through your employees that they are also invited to join your open enrollment meetings.

You can also invite them to view any electronic material you may post online, like the aforementioned videos.

If they cannot make a general meeting, you can invite them to come in to meet with your human resources manager if they have questions.

Remind them of the ACA

You can use open enrollment as a way to remind your staff of their responsibilities to secure coverage under the Affordable Care Act.

Let them know that employees that refuse affordable coverage from their employer and opt to purchase it on a public exchange will usually not be eligible for government premium subsidies.

Ask us about the most frequently asked questions about the ACA and we can help you prepare a list of online resources that they can access to get answers to those questions you may not be able to answer.

The meeting

Send out meeting notices early to give your employees time to prepare and set aside time. Try to make the meeting engaging with real-life examples and case studies.

You may want to consider video recording the session and also providing remote access to employees that don't work on-site.

Provide enough time for the main presentation as well as questions from your employees. ❖

Business E-Mail Compromise Scams Top Threat

BUSINESS E-MAIL compromise scams are now the most common type of cyberattack businesses face, and all types of these attacks are showing no signs of letting up, according to a new report.

Nearly three out of every four businesses were targets of these attacks and 29% of those firms became victims of successful attacks, according to the report by Arctic Wolf, a cyber-security firm.

While this has become the most common type of attack, a number of other schemes like ransomware attacks and data breaches continue growing in number.

Any of these attacks can drain a company's finances and result in tricky legal and possibly reputational issues that take time and money time to resolve.

The trends

The main threats businesses face, according to the report, are:

Business e-mail compromise (BEC) – Seven in 10 organizations surveyed said they had been targeted by these types of scams.

Some examples of BEC attacks include impersonating company executives to request wire transfers, falsifying invoice payment details, and tricking employees into revealing sensitive information. These scams can result in significant financial losses for businesses.

CAUTION: For businesses that use cloud-based e-mail services like Office365, these attacks are hard to detect since they don't reside on company servers.

With many organizations moving to cloud-based e-mail services, these types of attacks can be difficult to identify with traditional security tools and may go undetected until they have successfully executed their objectives.

Data breaches – Nearly half (48%) of organizations surveyed reported that they'd found evidence of a breach in their systems. The authors said that does not mean that the other 52% didn't suffer a breach; it means they failed to find evidence of one.

Ransomware – Some 45% of organizations surveyed admitted to being the victim of a ransomware attack within the last 12 months. These attacks usually involve criminals gaining access to a company's systems by getting an employee to click on a malicious link, after which they lock down the system and demand a ransom to unlock it.

Increasingly, perpetrators are also stealing data and demanding a second ransom to give it back and not release the data to others.

What you can do

How to Protect Against BECs

- Register all domain names that are similar to the business's legitimate website and can be used for spoofing attacks.
- Create rules that flag e-mails received from unknown domains.
- Monitor and/or restrict the creation of new e-mail rules on your servers.
- Enable multi-factor authentication.
- Conduct BEC drills, similar to anti-phishing exercises.
- Companies that use Office 365 or other cloud-based e-mail services, should employ detection tools or services specifically designed to monitor for threats related to BEC scams.

To combat ransomware:

Regularly back up system. Verify your backups regularly. This way you can restore functions if hit by ransomware.

Store backups separately. In particular, store backups on a separate device that cannot be accessed from a network, such as on an external hard drive.

Train your staff. Train your staff in how to spot possible phishing e-mails that are designed to convince an employee to click on a malicious link that will release the ransomware. ❖