ACRISURE®

June 2024 | Volume 12 | Issue 3

THE REPORT

Workplace Safety

Indoor Heat Illness Rules Likely Coming Soon

THE CAL/OSHA Standards Board has voted to approve new heat illness prevention regulations that will require some workplaces to make significant adjustments to their operations in order to comply, possibly starting early this summer.

The vote has been challenged, and at the last minute the California Department of Finance withdrew its approval of the regulatory changes due to a lack of full analysis on their potential financial impact on state entities, particularly state-operated correctional facilities.

However, Cal/OSHA is already in the process of creating a carveout for these entities to appease the Finance Department.

The indoor heat illness prevention standard applies to most indoor workplaces where the temperatures reach at least 82 degrees. According to Cal/OSHA, that includes facilites like warehouses, manufacturing and production facilities, greenhouses, wholesale and retail distribution centers, restaurant kitchens and dry cleaners.

The rules

Applicable employers will need to create and maintain a written indoor heat illness prevention plan that includes the following:

82-degree trigger – When temperatures indoors reach this level, employers must:

- Have and maintain one or more cool-down areas when employees are present, which must be kept at a temperature below 82 degrees.
- Allow and encourage staff to take preventive cool-down rests in a cool-down area when they feel the need. They should be monitored for signs of heat illness during rests.
- Provide drinking water near the areas employees are working.
- Observe all employees during heat waves when a workplace has no measures for controlling the effects of outdoor heat on indoor temperatures.

87-degree trigger – When the temperature exceeds 87 degrees, employers must measure the temperature and heat index, and identify all other environmental risk factors for heat illness. Firms must keep records of the temperature/heat index.

They must also implement control measures such as:

- Using air conditioners, swamp coolers, ventilation or other measures to reduce the air temperature (engineering controls);
- Adjusting work procedures, practices or schedules to minimize exposure to heat, such as changing shifts to start earlier and avoid the hottest parts of the day (administrative controls); or
- Using personal heat-protective equipment, such as water- or air-cooled garments or heat-reflective clothing.

Employers with affected workplaces must also observe new employees for 14 days when working under these conditions.

Emergency response – Employers must develop emergency response procedures, which must include:

- An effective communication system to allow workers to contact a supervisor or emergency services.

See 'Employers' on page 2

CONTACT US

Pleasant Hill Office
363 Civic Drive, 100
Pleasant Hill, CA 94523
Phone: 925-686-2860

Morgan Hill Office
15005 Concord Circle
Morgan Hill CA 95037
Phone: 408-842-2131

Sacramento Office
111 Woodmere Rd., Suite 290
Folsom, CA 95630
Phone: 916-970-2745

San Diego Office
5330 Carroll Canyon Rd, Suite 110
San Diego, CA 92121
Phone: 858-345-5787

License No. 0K07568

Groundbreaking Decision

New FTC Rule Bans Non-Compete Agreements

THE FEDERAL Trade Commission on April 23 approved a new rule that bans employers from requiring new employees to sign non-compete agreements. The rule will take effect in August 2024, after the commission voted 3-2 to approve it.

Besides banning future non-compete agreements, the new rule also nullifies all existing non-competes and requires employers to inform current and past employees that they will not be enforced.

Obviously, employers will need to scramble to comply with the new rule as the ramping up period is relatively short. However, it should be noted that the day after the regulations were announced, the U.S. Chamber of Commerce and other business groups filed lawsuits to block the rule from taking effect.

This new federal rule comes after four states — California, Minnesota, North Dakota and Oklahoma — banned non-competes and 13 others have laws limiting their use.

Under the FTC's new rule, existing non-compete agreements for the vast majority of workers will no longer be enforceable after its effective date.

Existing agreements for senior executives — who represent less than 0.75% of workers — can remain in force under the final rule. The rule defines senior executives as workers earning more than $151,164 annually and who are in policy-making positions.

That said, employers are banned from entering into or attempting to enforce any new non-competes, even if they involve senior executives.

Employers will be required to provide notice to workers other than senior executives who are bound by existing non-competes that they will not be enforcing the agreements.

The next step

Since the rule has already been challenged in court, a judge may put a stay on it while litigation proceeds, but employers can't count on that.

Time is quite short to prepare for the new rule. If you have any current non-competes, or if you require new employees to sign one, you should consult with your legal counsel to discuss your procedures going forward and the steps you'll have to take to comply with the new rule.

To help employers adhere to the requirement that they inform current and former employees that their non-compete agreements are null and void, the FTC has included model language in the final rule.

The commission said that employers have several alternatives to non-compete agreements that still enable firms to protect their investments without having to enforce a non-compete.

Trade secret laws and non-disclosure agreements both provide employers with well-established means to protect proprietary and other sensitive information. Researchers estimate that over 95% of workers with a non-compete already have an NDA. ❖

Continued from page 1

Employers Must Develop Emergency Response Procedures

- Steps for responding to signs and symptoms of heat illness, including first aid and providing emergency medical services.
- Emergency response procedures for severe heat illness.
- Monitoring employees exhibiting signs of heat illness, and not leaving them alone without offering them on-site first aid or medical services.

Training – Employees and supervisors will need to be trained on:

- Personal risk factors for heat illness.
- Their employer's procedures for complying with the regulations.
- The importance of frequent water consumption.

The takeaway

As mentioned, at this point there is no definitive date for these regulations taking effect, but Cal/OSHA insists they will be ready before summer starts in late June. ❖

Can Group, Private Disability Policies Work Together?

ACCORDING TO the Social Security Administration, a 20-year-old has more than a 25% chance of becoming disabled before reaching retirement age.[1]

Loss of income for such a duration has the potential to cause significant financial hardship. And while Social Security Disability Insurance may help, it's critical to understand that about two-thirds of initial applications are denied and the average SSDI payment is only $1,534 a month.[2,3]

Disability coverage may be available through your employer, who may pay all or a portion of the cost for your coverage.

Employer plans typically pay up to 50% to 60% of your income. This limited coverage might not be enough to meet your bills, which is why you may want to supplement employer-based coverage with a personal policy. Supplemental policies may be purchased to cover up to about 70% of your income.[4]

Taxation of Disability Benefits

When you purchase a personal disability policy, the benefit payments are structured to be income tax-free. Consequently, you may not be eligible for coverage that equals your current salary since your take-home pay is always less.

If your employer paid for your coverage, then the income you receive generally will be taxable.

If you paid for a portion of the employer-provided coverage, then the pro rata amount of the benefits you receive are structured to be tax-free.

Choices, Choices, Choices

Consider the waiting period before disability payments begin. A longer waiting period saves you money, but it also means that you may have to live off your savings for a longer period. You are the best judge of how much of this risk you are comfortable assuming.

You also may want to coordinate the waiting period with any short-term disability benefits you could have. For example, if your short-term disability covers you for 90 days, look to have at least a 90-day waiting period so that you can potentially lower the cost of the long-term policy.

Ask how a policy defines an inability to work. Some policies will say "the inability to do any job or task;" others will say "own occupation." You may prefer the latter definition so you're not forced to perform some less-skilled, lower-paid work. That type of work may not help you meet your bills.

.

Edward C. Rusnak
Joseph Yang
Sagemark Consulting
3000 Executive Parkway, Suite 400
P.O. Box 5154
San Ramon, CA 94583

Phone: (925) 659-0372
Fax: (925) 804-2472
E-mail: Edward.Rusnak@LFG.c

1. Social Security Administration, 2024
2. Disability-Benefits-Help.org, 2024
3. SSA.gov, 2024
4. Investopedia.com, July 23, 2023

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. ❖