News You Can Use

May 2022
Volume 10
Issue 5

HEFFERNAN INSURANCE BROKERS
Because You're Different

Workers' Compensation

Rating Bureau Recommends 7.6% Rate Increase

THE WORKERS' Compensation Insurance Rating Bureau of California is recommending that benchmark workers' compensation rates increase an average of 7.6%.

The proposal comes as the economy heats up and, typically during times of growth, workplace injuries also increase.

The recommendation, if approved by the state insurance commissioner, would affect all workers' comp policies incepting on or after Sept. 1, 2022. However, Insurance Commissioner Ricardo Lara last year rejected a proposed rate hike and instead ordered a cut.

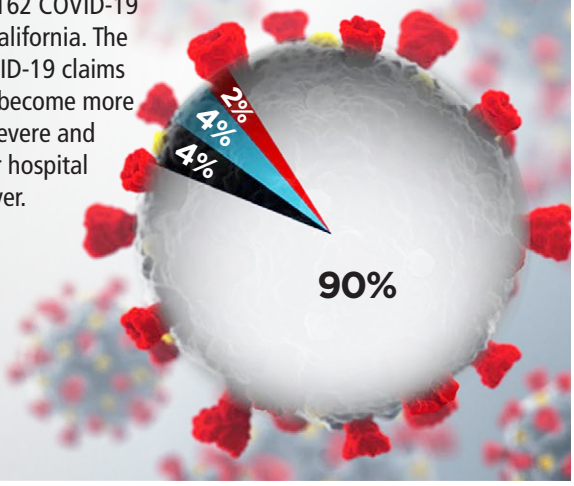
Also, the benchmark rates – also known as the pure premium rate – are only advisory and insurers are free to price as they feel fit.

Each workers' comp class code has its own pure premium rate.

THE COVID EFFECT ON WORKERS' COMP

As of Feb. 28, there had been 253,162 COVID-19 workers' compensation claims in California. The average medical payments on COVID-19 claims increase significantly as infections become more severe, and for those claims with severe and critical infections, the payments for hospital admissions were the main cost driver.

- **Mild** (no hospitalization)
- **Severe** (hospitalization, no ICU)
- **Critical** (with ICU care)
- **Death**



What's happening

The Rating Bureau says there are number of factors that are contributing to the increasing rates, including:

- An overall claims costs increase,
- Expected increases in the frequency of workplace injuries and claims,
- A rise in claims adjusting costs,
- Wage increases (part of workers' comp includes replacement of a portion of wages via temporary and permanent disability payments), and
- Expected future costs of COVID-19 workers' compensation claims.

Since the pandemic started, insurers have been barred from considering COVID-19 workers' comp claims when calculating an employer's claims history. But that exemption will come to an end on Sept. 1. So, the WCIRB is including a 0.5 percentage point provision for the projected costs of future COVID-19 claims in the coming year.

The effects of wage hikes are also expected to increase claims costs. Payouts for lost wages while sick workers recuperate are expected to rise more than 11% by 2024.

Medical costs per claim are projected to increase about 6.5% from $29,896 as of Dec. 31, 2021, to $31,847 at year-end 2024.

The next step

After the WCIRB submits the proposal to the Department of Insurance, the insurance commissioner will hold a hearing.

At that time, actuaries representing employers and labor will make counter-proposals, which are usually lower than the bureau's.

After that, the insurance commissioner can approve the proposal or reject it and order his own rate increase or decrease.

That's what happened last year, when the WCIRB proposed a 2.7% hike, and Lara rejected it and instead ordered a decrease of 3.3%.

And remember: A number of factors go into calculating your insurance rate, including your industry, your history of claims and your geographic location.❖

CONTACT US

If you have any questions regarding your coverage or our products, please call us at one of our offices:

Walnut Creek
San Francisco
Menlo Park
Portland
St. Louis
Petaluma
Los Angeles
Irvine
Seattle
Phoenix

Sales: 877-731-7905
Service: 800-234-6787
CA License No.: 0564249

Privacy Liability

Companies Bleed Data as Workers Move It Offsite

THE MORE employees are working from home, the greater the risk that their employers' sensitive data is also being stored on their poorly secured devices and laptops.

A new study by Symantec Corp. found many workers are sharing, moving and exposing sensitive company data as part of carrying out the requirements of their jobs, and they may not realize they could be compromising the information or that what they are doing is wrong.

More worrisome, the study found that half of all employees surveyed who left or lost their jobs in the prior 12 months had kept confidential company data. When that happens, the departing worker, your company and the new employer are all put at risk.

How Data Leaks from Your Firm

- Workers move it to their personal devices, both mobile and at home,
- Employees transfer the data or save it on cloud services or personal hard drives, or
- Employees take data with them to their new jobs.

Worse still, the majority of employees put these files at further risk because they don't take steps to delete the data after transferring it.

"In most cases, the employee is not a malicious insider," writes Symantec, "but merely negligent or careless about securing IP. However, the consequences remain. The IP theft occurs when an employee takes any confidential information from a former employer."

Why Data Leaks from Your Business

- 47% of employees say their organization doesn't take action when employees take sensitive information offsite.
- 68% say their employer does not take steps to ensure staff do not use confidential competitive information from third parties.
- 56% do not believe it is a crime to use a competitor's trade secrets.

What you can do

Symantec suggests attacking the problem from multiple angles:

- **Educate employees** – You should take steps to ensure that IP migration and theft awareness is a regular and integral part of security-awareness training. Create and enforce policies dictating how they can and cannot use company data in the workplace and when working remotely.

Help employees understand that sensitive information should remain on corporate-owned devices and databases. Also, new employees must be told that they are not to bring data from a former employer to your company.

- **Enforce non-disclosure agreements** – If you have not done so already, you need to craft new employment agreements to ensure they include specific language on company data.

They should include language that the employee is responsible for safeguarding sensitive and confidential information (and define what that is).

For employees that are leaving your employ, conduct focused conversations during exit interviews and make sure they review the original IP agreement. Include and describe, in checklist form, descriptions of data that may and may not transfer with a departing employee.

- **Track your data** – You need to know where your data is going and how you can find out by using monitoring technology. One option is to install data-loss-prevention software that notifies managers and employees in real time when sensitive information is inappropriately sent, copied or otherwise improperly exposed.

Also introduce a data-protection policy that monitors inappropriate access or use of company data and notifies the employee and you of violations.

This increases security awareness and deters theft. When you know how data is leaving your company, you can then take steps to prevent it from seeping out. ❖

Construction Sector

Inspections of Public Works Projects Increase

CONSTRUCTION COMPANIES and contractors that work on publicly funded projects in California can expect increased enforcement activity from a new task force that will target businesses that fail to comply with labor and workers' compensation laws.

The main focus of the Labor Enforcement Task Force is public works contractors, which the Department of Industrial Relations defines as prime contractors and subcontractors that work or bid on public works projects.

Targeting wrongdoers

The task force, which has been funded with $30 million thanks to legislation passed in 2021, includes representatives from a number of agencies under the DIR, which are pooling their resources and sharing information to ferret out employers that fail to:

- **Carry workers' compensation insurance.** All California employers are required to carry workers' comp insurance to cover their employees in case they are injured on the job.
- **Comply with Cal/OSHA standards.**
- **Comply with apprenticeship rules.** All public works contracts valued at $30,000 or more carry an obligation to hire apprentices, unless the craft or trade does not require the use of them, as indicated in the corresponding prevailing wage determination. You can check the prevailing wages for apprenticeships by county and job description here.
- **Comply with wage and hour laws and prevailing wage laws for public works projects**. Employers must pay all workers employed on qualifying public works projects the prevailing wage for their lines of work. Those prevailing wages are determined by the DIR according to the type of work performed and the location of the property.
- **Comply with skilled and trained workforce regulations for public works projects.**

Employers that fail to comply with public workers requirements can face civil penalties as well as criminal charges.The same goes for employers that don't carry workers' compensation coverage or underreport the number of workers they have in order to reduce the premium they pay.

And employers that fail to comply with Cal/OSHA safety requirements can be cited and fined for those infractions.

The Labor Enforcement Task Force, which operates under the direction of the DIR, is a coalition of enforcement agencies, including: Cal/OSHA, the Labor Commissioner's Office, and the Contractors State License Board and local agencies.

The stated goal of the task force is to combat the underground economy, which refers to any business which operates without following public work requirements, creates unsafe work conditions or attempts to gain an unfair economic advantage by skirting the law.

What you should do

Firms working on public works projects in California should take extra care to ensure they are complying with all applicable public works, workers' compensation and workplace safety laws.

Documentation is key to handling any audit that you are faced with. Keep good records of your safety efforts as well as your payroll and insurance. ❖

Growing Risk

Is Your Workplace Prepared for Violence?

IN 2020, more than 20,000 people were injured in workplace assaults; almost 400 died. The number of workplace injuries and fatalities from violent incidents has climbed steadily over the past decade.

While some workplaces, such as health care facilities, are at greater risk than others of these incidents, no workplace is immune. Advance preparation for and prevention of such violence has never been more important than it is today.

How can an employer prepare for the unthinkable? Workplace safety experts advise several measures:

- **Assess the risk** – In which departments and locations in the workplace are attacks most likely to occur? It could be the human resources department, where employees may be subject to disciplinary action. It could be the reception area where random members of the public enter the premises. Or it could be the offices of the company's upper managers.
- **Form a threat management team** – These will be the people that other employees look to during an event to manage and possibly defuse the situation or summon help. They should be individuals who can be counted on to remain calm during a crisis, and they should come from different departments within your organization.
- **Create a plan** – This does not have to be created out of thin air; there are plenty of resources employers can draw from. The Occupational Safety and Health Administration offers sample prevention and employee training programs. The Society for Human Resources Management offers its members a toolkit, and even the FBI has a guide to preventing workplace violence.
- **Train employees on how to recognize potential threats, actual incidents** – The federal Department of Homeland Security provides many resources to help prepare employees for active shooter situations. Their program educates workers on behavioral indicators of potential violence, possible attack methods, emergency action plans, and what to do during an incident.

Look for warning signs

Employees should be trained to watch for warning signs of a potential for violence in their co-workers, including:

- A history of troubling behavior.
- Sudden changes in behavior.
- Interpreting their perceptions as reality.
- Showing a desire to take or regain control.
- Listening only to information that confirms their beliefs.

You should implement policies encouraging employees who notice these warning signs to discuss them with a manager or an HR staff member. Another option is to implement an anonymous tip line for reporting troubling behavior.

In case of emergency

In addition, employees should be trained to react in specific ways should a workplace violence incident erupt:

- **Run** – If feasible without putting themselves in more danger, they should leave the premises through the nearest available exit. Employers should clearly inform employees of the exits' locations.
- **Hide** – If vacating the premises is not feasible, take cover in a place out of the attacker's view.
- **Fight** – As a last resort, attempt to disable the attacker. However, this may increase the danger to the employee.

The takeaway

No amount of preparation will protect an organization with 100% certainty against workplace violence.

However, thoughtful analysis and planning, coupled with employee training, can make these incidents less likely to occur – and make the ones that do occur less severe. It is an unfortunate fact of the times we live in, but organizations of all sizes need to prepare for the possibility of assaults in their workplaces.❖