MINDFUL
INSURANCE SOLUTIONS INC.

RISK REPORT

APRILI 2020 | VOLUME 3 | ISSUE 2

Law Requires Paid Sick Leave, FMLA Benefits

LEGISLATION SIGNED into law by President Trump extends sick leave benefits for workers who are stricken by the coronavirus, as well as provide for additional weeks of time off under the Family Medical Leave Act so they can be guaranteed of being able to return to their jobs afterwards.

Employers need to pay extra attention to the added paid sick leave and FMLA provisions of this new law, the Families First Coronavirus Response Act, which only applies to employers with fewer than 500 employees.

Paid sick leave

Employees are entitled to two weeks (80 hours) of paid sick time for coronavirus-related issues.

Eligible workers must be paid their regular pay, up to $511 per day and $5,110 in total.

Those caring for someone subject to quarantine due to COVID-19, and parents of kids who can't go to school or daycare, will receive two-thirds of their regular pay, up to $200 daily with a $2,000 cap.

The emergency sick leave benefit can be used immediately, regardless of how long the worker has been employed with you.

The law does not require certification of an order by government or a health care provider. But employers can require reasonable notice procedures, such as not announcing in the middle of a shift that they take COVID-19 sick leave. They cannot require the employee to find a replacement worker to cover the shifts they will miss. Employers must post the law's requirements "in conspicuous places."

Employers are not allowed to discipline a worker who takes this sick or FMLA leave for coronavirus purposes. If an employer refuses to provide the leave, they can be subject to paying back pay and statutory damages.

Important: This law provides payroll tax credits to offset costs of providing paid leaves.

PAID SICK LEAVE RULES

Paid sick leave can be used when an employee cannot work or telecommute if:

- They are subject to a government quarantine or isolation order related to COVID-19;
- They have been told by a health care provider to self-quarantine due to COVID-19;
- They have symptoms of COVID-19 and are seeking a medical diagnosis;
- They are caring for an individual subject to quarantine due to COVID-19;
- They need to care for a child whose school or daycare is closed due to coronavirus.

FMLA

The law provides for 10 additional weeks of FMLA leave, but only for those who must stay at home to care for a child whose school is closed or their childcare provider is unavailable due to COVID-19-related issues.

These 10 weeks will be paid at two-thirds the employee's regular rate of pay, up to $200 per day with a cap of $10,000. They will also receive 12 weeks of leave with job protection, though employers of health care or emergency care providers can exclude such employees.

The employee would likely use up their two weeks of paid sick leave before applying for FMLA benefits, which unlike traditional FMLA (which is unpaid), are paid leaves after the first 10 days under the new law.

Employees who have been working for more than 30 days are eligible, and the employer can require them to provide

See 'Law' on page 2

CONTACT US

MINDFUL
INSURANCE SOLUTIONS INC.

7750 COLLEGE TOWN DRIVE,
SUITE 101 SACRAMENTO, CA 95826

Toll Free: 877-223-4437
Fax: (530) 419-4811

E-mail: info@mindfulins.com

License #0I67525

Keeping Operations Going

Tips for Successful Telecommuting

WITH THE current isolation orders for most workers in California, many companies have had to scramble to put systems in place to allow their employees to telecommute.

Many businesses are not set up for having employees work from home, and they have legitimate concerns about productivity and communications. But there are steps you can take to make sure that you keep your employees engaged and on task.

1. Make sure they have the right technology

If you don't already have one, you may want to consider setting up a company VPN so your employees can access their work e-mail and databases. You will also need to decide if you are going to provide them with a company laptop, and you need to make sure that they have an internet connection that is fast enough to handle their workload.

Also provide an infrastructure for them to be able to work together on files. If they are not sensitive company documents, they can use Dropbox or Google Documents, which allow sharing between co-workers.

2. Provide clear instructions

It's important that you provide clear instructions to remote workers. Some people do not perform well without direct oversight and human interaction. Without that factor, you will need to spell out your expectations and the parameters of the projects they are working on in detail.

Make it clear that if they are confused or unsure about any part of the work, they should contact a supervisor for clarification. If you can eliminate misunderstandings, then your workers can be more efficient.

3. Schedule regular check-ins

To hold your employees accountable for being on the clock, schedule calls or virtual meetings at regular intervals. Even instant messaging works. During these meetings they can update their superiors on their work. This also helps with productivity, since there are consequences for failing to meet expectations and coming to the meeting empty-handed.

Their supervisors should be working when they are, so they can be in regular communication.

4. Keep employees engaged

One of the hardest parts of working from home is the feelings of isolation and detachment from colleagues. It's important that you build in interactive time for your workers.

One way to do that is by using a chat program like Slack, Hangouts or WhatsApp (which has a group chat function). For remote workers, these programs are a blessing because they make it easy to keep in touch with their colleagues in and out of the office – and they level the playing field, so to speak, by making distance a non-issue.

5. Cyber protection

With employees working from home, you also increase your cyber risk exposure, especially if they are using a company computer that is tapped into your firm's database or cloud.

Teach them cyber security best practices, such as:

- Not clicking on links in e-mails from unknown senders.
- Making sure their systems have the latest security updates.
- Backing up their data daily.
- Training them on how to detect phishing, ransomware and malware scams, especially new ones that try to take advantage of people's fears about COVID-19.

The takeaway

If you've not had staff telecommuting in the past or are asking many employees who never have worked in that way to telecommute, there will be some growing pains as you work out the kinks.

If you follow the above tips, it will make the transition easier for your workers, their managers and the organization as a whole.

Continued from page 1

Law Only Applies to Employers with Fewer Than 500 Workers

reasonable notice that they are taking leave.

A final word

This law only applies to employers with fewer than 500 workers, so it leaves uncovered those people who work for larger companies.

Also, employers need to make financial plans, as the credit cannot be claimed until after the employer pays their payroll taxes.

A bigger issue is that the law requires that workers be paid the sick leave even if they are not sick, but have been ordered to self-isolate. In states that have ordered workers to self-isolate, such as California, employers could be faced with an avalanche of paid sick leave claims all at once.

This law sunsets on Dec. 31, 2020.

CARES Act

New Law Helps Coronavirus-hit Employers, Workers

THE $2 TRILLION Coronavirus Aid, Relief, and Economic Security (CARES) Act stimulus law has a number of provisions that employers and their workers need to know about and can take advantage of during this crisis.

The CARES Act aims to help workers and employers weather the outbreak by:

- Extending unemployment benefits.
- Requiring health plans to cover COVID-19-related costs.
- Providing Small Business Administration (SBA) emergency loans.
- Providing emergency loans for mid-sized and large companies.

Parts of the CARES Act will likely benefit your organization and employees in some way. Here's what you need to know:

Extended unemployment

The CARES Act extends unemployment insurance benefits to workers, as long as they lost their jobs due to the outbreak.

Unemployment benefits under the CARES Act also apply to furloughed employees.

Workers in California will be able to collect both state unemployment and federal unemployment through the new law.

Under existing state law, workers who have lost their jobs can already receive regular unemployment benefits of between $40 and $450 per week, depending on their highest-earning quarter in a 12-month period beginning and ending before they apply for benefits with the state Employment Development Department. These benefits can last for up to 26 weeks.

The Pandemic Emergency Compensation program funded by the new law will provide an additional $600 per week on top of state unemployment benefits, through July 31.

The law extends state-level unemployment by an additional 13 weeks. For example, whereas most of California's unemployment benefits last 26 weeks, the bill extends state benefits to 39 weeks.

The extended benefits will last through Dec. 31.

Health plan changes

Under the CARES Act, employer-sponsored group health plans must provide for covered workers – without cost-sharing or out-of-pocket expenses – the cost of COVID-19 testing, treatment and vaccinations when and if they become available.

SBA loans

In response to the Coronavirus (COVID-19) pandemic, small business owners are eligible to apply for an Economic Injury Disaster Loan advance of up to $10,000.

This advance will provide economic relief to businesses that are currently experiencing a temporary loss of revenue. Funds will be made available following a successful application. This loan advance will not have to be repaid.

This program is for any small business with fewer than 500 employees (including sole proprietorships, independent contractors and self-employed persons) as well as private non-profit organization affected by COVID-19.

You can find more information here.

And the law's Paycheck Protection Program, offers 1% interest loans to business with fewer than 500 workers.

Borrowers who don't lay off workers in the next eight weeks will have their loans forgiven, along with the interest.

These loans are designed to provide a direct incentive for small businesses to keep their workers on the payroll. If small businesses maintain payroll through this economic crisis, some of the borrowed money via the PPP can be forgiven – the funds will be available through June 30. Act fast.

Mid-sized employers

Under the new law, the Secretary of the Treasury is authorized to implement financial assistance programs which specifically target mid-size employers with between 500 and 10,000 employees.

Loans would not have an annualized interest rate higher than 2% and principal and interest would not be due and payable for at least six months after the loan is made. But unlike loans under the PPP, these are not forgivable.

Cyber Security

Malicious Coronavirus-related E-Mails Spread

AS IF BUSINESSES didn't have enough to worry about, online scammers have started sending out malicious e-mails to organizations about coronavirus that appear to be from business partners or public institutions.

The criminals send these to rank and file employees in the hope that at least one of them will click on a link or attachment in the e-mail, which unleashes malware or tries to trick them into wiring money for supplies purportedly to protect the organization's workers.

The number of malicious e-mails mentioning the coronavirus has increased significantly since the end of January, according to cyber security firm Proofpoint Inc. The company noted that this wasn't the first time they had seen such widespread cyber attacks associated with some type of disaster. But because this is global in nature, it decided to track the new threat.

This practice of launching cyber attacks that are centered around global news and outbreaks (like the current COVID-19 coronavirus) isn't anything new. Cyber criminals have long employed these tactics to take advantage of users' desires to keep as up to date with any new information as possible, or to evoke powerful emotions (like fear) in the hope that their sentiments will get the better of them and they will not pause to check for the legitimacy of these e-mails.

The cyber criminals are using the public's ignorance about coronavirus, as well as the conflicting claims of how to protect against it, to lure people into clicking on their malicious links or get them to wire money. Because people are afraid, their guards may be down and they may not be as careful about identifying the e-mail as dangerous.

Some real-life examples

- Japanese workers were targeted in January and February with e-mails that looked like they came from local hospitals. The messages even included legitimate contact information for key personnel.

The e-mails were focused on employees of various companies and came in a message that would look like it's a reply to something, or a warning that people are getting from the government. But when they clicked, it was malware.

- E-mails were sent to companies in the transportation sector that looked like they came from an employee of the World Health Organization. They included the WHO logo and instructions about how to monitor crews aboard ships for coronavirus symptoms, and they included an attachment with instructions.

This phishing e-mail attack was intended to lure individuals into providing sensitive data, such as personally identifiable information and passwords.

- Companies in the US and Australia have been receiving malicious e-mails that use a display name of "Dr Li Wei" and are titled "CORONA-VIRUS AFFECTED COMPANY STAFF."

What you can do

All that it takes to break into your business is a cleverly worded e-mail message. If scammers can trick one person in your company into clicking on a malicious link, they can gain access to your data.

It's important to train your staff to identify suspicious e-mails. They should avoid clicking links in e-mails that:

- Are not addressed to them by name, have poor English, or omit personal details that a legitimate sender would include.
- Are from businesses they are not expecting to hear from.
- Ask you to download any files.
- Take you to a landing page or website that does not have the legitimate URL of the company the e-mail is purporting to be sent from.
- Include attachments purportedly with advice for what to do. Do not open them even if they come from relatives or friends.