October 2021, Volume 10, Issue 10

Curry Insurance Agency

WORKPLACE SAFETY

Permanent COVID-19 Standard Coming Soon

NO MORE DEEP CLEANING: *The permanent standard eliminates rules regarding cleaning and disinfecting procedures in the workplace.*

CAL/OSHA has taken the first step towards creating a semi-permanent COVID-19 standard to replace the emergency temporary standard that currently governs workplace coronavirus prevention measures in the state.

On Sept. 17, Cal/OSHA released a discussion draft for permanent COVID-19 regulations to give stakeholders the chance to comment on it before it starts work on writing the regs.

Even though they are "permanent," the rules would be subject to renewal after two years from the effective date or they would expire if the threat has receded by that time.

Elements of the draft standard

Here's what the draft standard would do:

Follow CDPH rules – Require that employers follow California Department of Public Health COVID-19 prevention orders.

Masks for unvaxxed staff – Unvaccinated staff must wear masks. Employers must provide masks fwhen the CDPH requires them.

Outbreak rules – During an outbreak in the workplace, all staff would be required to wear face coverings regardless of vaccination status. Employers would need to provide respirators during major outbreaks to all employees.

No COVID-19 Prevention Plan – Employers would not need to have a COVID-19 Prevention Plan, as required in the temporary emergency standard. Instead, they would be required to address COVID-19 prevention strategies in their Injury and Illness Prevention Plan.

Masks for at-risk staff – Require employers to provide N95 respirators to employees who have been identified by a doctor as being at increased risk of severe illness from COVID-19, regardless of their vaccination status.

'Fully vaccinated' defined – Define a "fully vaccinated employee" to mean that the employer has a copy of their vaccination record that includes the vaccine maker and date of the last dose.

Retaining records – Require employers to keep COVID-19 vaccination records for two years after the period requiring them to keep the records ends. That means if the rule sunsets in a few years, employers would be required to keep those records for another two years.

Testing rules – Require that employers provide COVID-19 testing to all employees who have come into close contact with another team member who has tested positive for the virus. Testing must be provided at no cost to the employee.

No paid leave for infected staff – Eliminate the provision for paid leave for workers who contract the coronavirus.

Handwashing and cleaning – Eliminate rules regarding handwashing and cleaning and disinfecting procedures in the workplace.

The takeaway

If you have been following Cal/OSHA's emergency temporary standard, you should continue to follow the current requirements.

The new rules simplify the emergency standard and are easier to abide by, particularly concerning the requirement that COVID-19 prevention plans can be included in your IIPP rather than in a separate document. ❖

CONTACT US

Curry Insurance Agency

If you have any questions regarding any of these articles or have a coverage question, please call us at:

ISU Curry Insurance Agency
489 E. Colorado Boulevard
Pasadena, CA 91101
Phone: 626-449-3870
Fax: 626 449-5268
License No. : 0588757

CYBER SECURITY

Is Your Data Secure on Your Workers' Phones?

WITH ABOUT 75% of employees in the U.S. using their own devices for work communications and productivity, businesses must implement safeguards to keep company data from being compromised should a device be stolen, hacked or hit by a virus.

But, while a company can install certain software and make security settings on its own phones, the task is harder when your workers want to use their own devices for their jobs, according to a new study by mobile solutions provider CDW.

Fortunately, the market has responded with systems and software to help businesses secure the personal smartphones and tablets that their employees use to conduct their jobs.

Benefits of BYOD

There are a number of benefits to allowing your staff to "bring your own device" (BYOD), according to the CDW report, including:

- **More employee satisfaction** – It allows them to choose the phone they prefer, and requires them to keep one device.
- **Increased productivity** – When your employees have access to your company's resources, they can do their work from anywhere that is convenient.
- **Cost savings** – You won't be shelling out for phones and cell phone plans, although you may need to pay for various security platforms.
- **Disaster recovery** – If disaster strikes, your staff can work remotely with their smartphones.

Also, because employees are likely to have their phone plans through a variety of carriers, if one carrier goes down in a disaster others may still be operational.

Risks

Increased mobility comes with more risk to your company's data or the information you store on your customers. When employees co-mingle personal and business uses on the phone it poses risks, particularly if the device is compromised and passwords discovered.

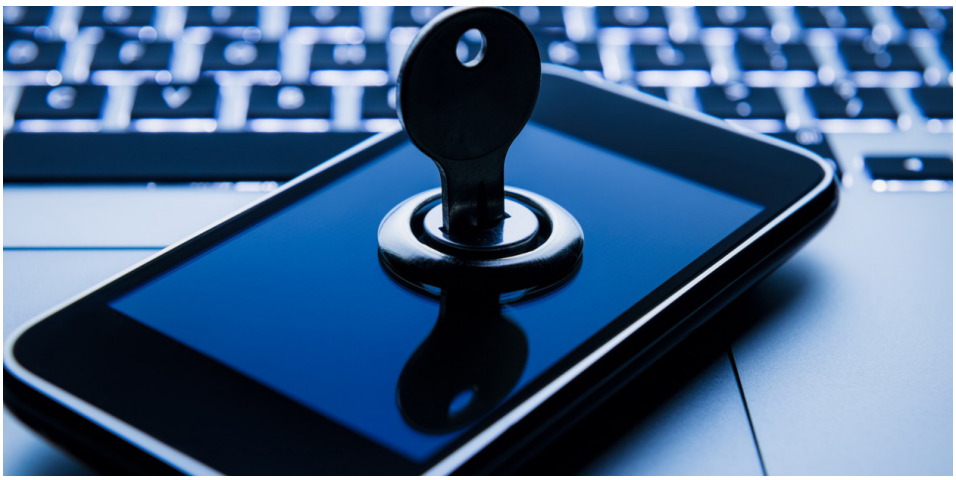
The biggest concern is hackers gaining access to an employee's personal files and using them as a gateway to your company's data.

This is made particularly easy if an employee uses the same password for both work and personal accounts.

Locked and loaded

The best weapon currently available for BYOD devices is what is known as Enterprise Mobile Device Management software.

Once the software is installed on your employee's phone, it gives you the ability to set the security configurations for the device remotely.



Other measures you can implement include:

- **Host-based firewalls** – These are installed on the phone and can help detect and stop viruses, malware and other malicious scripts.
- **Mobile web security** – Many mobile phone browsers include security controls that can help thwart unwanted programs and viruses from getting a foothold as a result of an errant click on a bad link.

The takeaway

If your staff are using their phones for work and they have enterprise apps that can access your databases, you may be putting your systems and intellectual property at risk in case their device is hacked, stolen or otherwise compromised.

If you follow the above advice, you'll be better able to thwart any attacks on your employees' smartphones that could hamstring your business. ❖

Mobile Device Management Capabilities

- The ability to prevent data from being saved to removable media that are outside the organization's control.
- The ability to restrict access to software, such as preventing use of the organization's data on a device with applications which the company has not approved for use.
- Encrypting the business's data stored on a device, to stop unauthorized applications and users from accessing it.
- The ability to monitor each device's security settings, in order to detect violations of the firm's security policies.
- The administrator can remotely lock a device if it has been stolen or lost. This will keep anybody without knowledge of the unlock password from using the device.
- The administrator can remotely issue a command and all of the organization's data and applications will be wiped from the phone.

EMPLOYMENT PRACTICES

Employees Can Sue You If Customers Harass Them

WITH CONFRONTATIONS between angry customers and employees increasing during the COVID-19 pandemic, employers need to have policies in place to protect workers who are confronted.

Many customer-facing companies – retailers, restaurants, etc. – have seen an uptick in customers sexually harassing employees or racially attacking them. Even workers who don't interact with customers or vendors face to face can be be harassed: on the phone, through text messages or social media.

But there is also a larger risk to your organization: If you are not doing all you can to protect your staff against harassment by customers or vendors, you could be sued for those failures.

The typical employment practices liability insurance (EPLI) policy only covers costs related to claims of harassment, discrimination and other workplace ills perpetrated by company insiders. It won't cover complaints about customer or vendor harassment. But, there is a rider that will cover these claims: third party EPL coverage.

To protect your company from an employee lawsuit, you must first safeguard your workers.

SHOCKED: *Customers can even harass your staff via phone calls, text messages and e-mails. If an employee complains and you don't act, you could be setting your firm up for being sued.*

Training

You should implement policies and procedures that address discrimination and harassment issues, both from the standpoint of an employee's actions and the actions of third parties.

What Policies, Training Should Cover

- How employees should handle the situation when a customer is harassing or threatening them, including de-escalating techniques.
- Procedures for employees to report harassment.
- Having staff experiencing harassment say a safety word to a nearby worker to alert them of the situation, so another worker or manager can take their place or intervene.
- Encouraging staff to report to their manager if a certain customer continues harassing them each time they come in.
- Emphasizing the fact that you won't retaliate against staff who complain about a threatening client or vendor.
- Calling law enforcement if a customer's anger and actions are escalating.
- Training your employees to walk to their cars in groups after their shifts for safety reasons after a confrontation during their shift.

Employees must be periodically retrained through departmental meetings. To maintain the effectiveness of departmental training sessions, be sure that supervisors are provided with copies of all policy updates and procedural changes.

Insurance

Insurance companies are increasingly requiring employers to implement discrimination and harassment prevention policies and employee training on the subject before they will issue a policy.

An employer is liable for third party harassment or discrimination just as it would be for harassment by a co-worker – that is, the employer is liable if its behavior regarding the harassment is negligent.

Negligence means that the employer knew or should have known of the harassment and failed to take appropriate corrective action.

As mentioned, a typical EPLI policy won't cover your legal expenses, settlements or court judgments if the harasser is a customer or vendor. For that you would have to purchase third party EPLI.

These policies cover your firm if you're sued by an employee over:

Harassment by an outsider. This can include unwanted sexual advances or requests for sexual favors. Both verbal and physical conduct, as well as other forms of harassment that create a hostile or offensive work environment, are covered. Some policies also cover accusations of mental anguish, emotional distress, humiliation and assault.

Discrimination by an outsider. This includes discriminatory practices against one of your staff based on their race, religion, age, sex, national origin, disability, pregnancy or sexual orientation (such as a customer refusing to be served by someone because of their race).

In some cases, EPLI carriers may not provide third party coverage to firms with a high potential for claims. Instead, they might offer limited coverage, like accusations of discrimination, but not harassment claims.

If you have staff dealing with customers regularly, this kind of insurance can protect your firm in case you are sued by a staff member for not doing enough to prevent customer harassment or discrimination. ❖

Produced by Risk Media Solutions on behalf of ISU Curry Insurance Agency. This newsletter is not intended to provide legal advice, but rather perspective on recent regulatory issues, trends and standards affecting insurance, workplace safety, risk management and employee benefits. Please consult your broker or legal counsel for further information on the topics covered herein. Copyright 2021 all rights reserved.

WORKPLACE SAFETY

OSHA to Issue Large-Employer Vaccine Mandate Rule

THE BIDEN administration has announced plans to mandate businesses with 100 or more employees to require their workers to be vaccinated for COVID-19 or be tested for the coronavirus on a weekly basis.

The order is part of a sweeping six-part "Path Out of the Pandemic" plan, which focuses on expanding vaccinations, opening schools safely, improving care for coronavirus patients and protecting the economic recovery.

'Path Out of the Pandemic' Plan

- Requires federal workers and federal contractors to be vaccinated.
- Requires health care workers in hospital settings that see Medicare and Medicaid patients to be vaccinated.
- Requires employers to give staff time off to get vaccinated.
- Calls on large entertainment venues to require proof of vaccination or a negative COVID-19 test for entry.

Employers are obviously concerned about the impending rules, particularly how they will be enforced and how to handle employees that opt for weekly testing or who refuse to be vaccinated based on religious or health reasons.

Since the order will be an emergency temporary standard (ETS), expect OSHA to issue the new rules within 30 to 60 days after President Biden's Sept. 9 announcement.

What to expect

An ETS can only remain in effect for six months, after which it has to be replaced by a permanent standard or sunset.

OSHA has already started work on the rule that the administration says "will require all employers with 100 or more employees to ensure their workforce is fully vaccinated or require any workers who remain unvaccinated to produce a negative test result on at least a weekly basis before coming to work."

Employment law attorneys say that depending on how the new rules are written, it may be a burden on many employers to collect and track weekly test results for those workers who choose not to be vaccinated. The added bookkeeping headache may prompt some employers to abandon it and impose a mandatory vaccine policy.

Weekly testing also costs money. California has a law that has been on the books long before the pandemic that require employers to pay for mandatory medical tests or reimburse employees who pay for those tests themselves.

Also, the Fair Labor Standards Act requires employers to pay employees for time spent undergoing testing during the workday or for time used on their days off to get tested.

Also, it's expected that the ETS will require employers to accommodate workers who won't get vaccinated based on medical issues or due to a "sincerely held religious belief."

There are still many questions that employers have:

- How will the 100-employee threshold be counted?
- How will employers collect proof of vaccination?
- What type of COVID-19 tests will be acceptable?

What you can do now

If you employ 100 or more people, you can get an early start by encouraging your employees to get inoculated against coronavirus. That way, when the rule comes into effect, you'll have a good start.

You should also decide if you want to allow employees to forgo vaccination and instead be tested.

Larger employers should regularly check for new guidance on unsettled issues such as:

- Whether the employee count will include part-time, full-time and temporary workers,
- Who will bear the financial costs for weekly testing, and
- Whether time spent obtaining a test and awaiting results is compensable time. ❖