



# Curry Insurance Agency

## WORKERS' COMP

# Drug Testing of Injured Workers Skyrockets

**D**RUG TESTING of injured workers by treating doctors has skyrocketed as physicians and insurers try to stop painkiller abuse and monitor patients for staying with their prescribed drug regimen.

The use of urine drug testing on injured workers in California increased 2,431% between 2007 and 2014, according to the California Workers' Compensation Institute (CWCI).

During that period, urine drug tests grew from 10% to 59% of all workers' compensation laboratory services, while drug test reimbursements increased from 23% to 77% of all lab payments in the system.

The main reason is to detect abuse of high-strength prescription pain meds known as opioids, and similar drugs.

Opioids can greatly increase the time an injured worker is away, as well as the cost of the claim.

Also, doctors are increasingly using the tests to ensure injured workers are taking the medicines they prescribe.

The downside is that the cost of the testing continues to increase and can easily be a few thousand dollars, adding significantly to the cost of claims.

Not only are more injured workers being tested, but they are being tested more often.

Here are other findings from the study:

- Among the injured workers who were drug tested, the average number of tests per employee more than tripled from 4.5 in 2007 to 14.9 in 2014, driving the average amount paid per date of service from \$96 to \$307 – a 220% increase.
- The number of providers who were paid for testing injured workers climbed from 428 in 2008 to 876 in 2014. Much of that growth is attributed to a migration towards physician in-office testing, because testing equipment has drastically come down in price.
- The amount paid for drug tests in California workers' comp is based on Medicare billing rules. These rules were revised in 2010 and 2011, after Medicare determined there were questionable billing practices for drug tests taking place.

The CWCI study found that after those changes were made, the mix of tests used on injured workers changed to avoid application of the fee schedule. That has increased the cost of testing.

### Is it necessary?

Several medical treatment guidelines call for doctors prescribing opioids to also test for illicit drug use under certain circumstances, such as when addiction or abuse is detected or when patients are at risk for overdose and death, sources said.

Doctors need to identify patients abusing drugs to avoid providing them opioids and change the treatment required for them.

Proponents say it helps keep injured workers' medicinal intake in check to ensure they are sticking with their drug regimens and also not abusing prescription pain medications.

Tests revealing that patients are using drugs for other than "clinical health" can also help workers' comp payers arguing before a judge or hearing officer regarding their responsibility for the claimant.

The purpose of testing is to assist in medical management.

Still, testing should be done based on medical necessity related to a claimant's medical presentation, dispensed drugs and evidence-based medicine protocols. ❖



CONTACT  
US



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  
Pasadena, CA 91101  
Phone: 626-449-3870  
Fax: 626 449-5268  
License No. : 0588757

## SECURITY CONCERNS

# Mobile Threat Booms: Revisit Your BYOD Policies

**W**ITH THE amount of new malware that targets mobile devices growing exponentially, if you have not set down rules for employees who use their own smart phones for company business, you should do so now.

Network security firm PandaLabs has reported that in the second quarter of 2015, it saw an average of 230,000 new types of malware every day and a total 21 million new threats.

Worse, cyber-criminals are creating improved malware variants that evade detection by antivirus software and apps.

Attacks on mobile devices are increasing even faster, says the report, with not only an increase in malware for the Android mobile platform, but more and more ransomware being developed for the iPhone platform.

Don't think it's a threat? In 2014, for the first time, Android devices were infected at the same rate as computers running the Microsoft Windows operating system.

It's estimated in the "Motive Security Labs Malware Report", by Alcatel-Lucent, that some 16 million devices are infected by malware.

With mobile device malware infections growing, you may need to re-evaluate your company's bring-your-own-device (BYOD) policies and the way security standards address personal phones, tablets and other Internet-connected machines in the workplace.

Mobile device malware will hit small and midsize businesses harder because of the popularity of BYOD in firms with smaller budgets and IT staffs.

Up until now, most company's BYOD security policies have focused on lost devices, password protection and the use of public Wi-Fi when transmitting sensitive data.

Even policies that include the installation of anti-malware software to the device do not completely address the mobile malware problem, according to the IBM-operated technology news website *PivotPoint*.

*Information Age* magazine recommends the following policies:

- **No unauthorized downloads** – Warn against downloading apps from unknown sources.
- **Use with care** – Inform your BYOD users that they need to be more cognizant of their online behavior. You will need to be creative in how you educate your employees about the risks of mobile malware.
- **Keep a register of connected devices** – As the IT team connects personal devices to the company network, they should also keep a record of the user and their device details. By maintaining a detailed register, companies can audit their company network regularly to detect unauthorized connections and resource usage.
- **Enforce on-device security** – Smart phones and tablets come with passcode controls that restrict access. As part of an employer's default BYOD agreement, staff should be expected to have the passcode enabled before they are granted access to corporate resources.
- **Use existing network tools more intelligently** – Many common network tools and services have functions that make it easier to manage mobile devices. Microsoft Exchange can be used to perform remote data wipes on stolen devices, for example. Make full use of these tools to automate common mobile device management tasks and to manage network logons, for instance.
- **Force VPN use** – To ensure that data transfers are secure in transit, require that your staff devices be set up with VPN access.
- **Mobile device management (MDM) platform** – An MDM platform allows you to enroll devices, specify and enforce network access rights and even apply content filtering.

### Insurance

Finally, your firm should look into cyber liability insurance, which can cover costs related to a cyber breach. ❖



## El Nino Alert

# Flood Insurance Can Save Your Firm from Calamity

**W**ITH FORECASTERS predicting significant rainfall thanks to the El Nino weather phenomenon, you could be putting your business at risk if you are not properly insured.

The average commercial flood claim is \$89,000, according to the National Flood Insurance Program.

And 25% of businesses that shut down after events such as floods never reopen.

Damage from flooding, including flooding generated by hurricane-generated storm surge, typically is not covered under a standard commercial policy, including a Commercial Package Policy or a Business Owners Policy.

Business located in flood plains will usually carry some flood insurance, but 30% of all floods in the U.S. occur outside flood plains. With record amounts of rainfall expected in the coming months, many firms' property may be at risk.

When evaluating whether you need flood insurance, consider your expectations and your needs. In many aspects, flood insurance differs greatly from other coverage for your business. Here are the major issues, according to the Insurance Information Institute:

### What does flood insurance cover?

Flood insurance covers damage to your building and contents caused by flooding.

This includes losses resulting from water overflowing from rivers or streams, heavy or prolonged rain, storm surge, snow melt, blocked storm drainage systems, broken dams or levees, or other similar causes.

Also, damage from mold and mildew resulting from the after-effects of a flood is covered, but each case is evaluated on an

individual basis.

Mold and mildew conditions that existed prior to a flooding event are not covered, and after a flood, the policyholder is responsible for taking reasonable and appropriate mitigation actions to eliminate mold and mildew.

Generally if water comes from above – for instance from rain or melting snow overflowing gutters and leaking onto your inventory – you'll be covered by your standard commercial property insurance.

### What's my risk for flooding?

This is a key question, of course. By far the best indicator for the risk you face is location: Is your business near the coast or a river, lake or stream?

What's the weather like? Is there a threat of hurricane, tornado or severe storm?

Is the business – and its primary equipment and inventory – on the bottom floor of the building or higher up, where it would be safer?

### Coverage Limits

Commercial flood insurance typically provides up to \$500,000 of coverage for your building and up to \$500,000 for its contents.

You can purchase what's called excess insurance coverage to rebuild properties valued above those limits, and this type of coverage usually includes protection against business interruption.

### Think ahead

Don't wait too long. Most flood policies won't take effect until 30 days after the purchase, so you can't wait until a threat surfaces to

We can assist you in evaluating if your business property is located in risk area and if you may need to secure flood insurance.

**CALL US TODAY!**



## EXCESS LIABILITY

# As Risks Rise, You Need a Commercial Umbrella

**A**S A RESPONSIBLE business owner you no doubt make sure that you are properly insured for any liabilities resulting from damage to other parties.

The costs of a large financial settlement could surpass the primary liability limits of your existing insurance policies, leaving your business responsible for the rest of those costs. And a high-cost accident or lawsuit could potentially put your company out of business.

### DANGEROUS SCENARIOS

- What if a visitor trips and falls at your business, breaking a leg and is unable to work for a few months while they recover?
- What if a customer suspected of stealing later proves their innocence and sues for defamation of character?
- What if one of your employees, driving a company truck, rams into a passenger car and severely injures some of the occupants?



### Unfurling the Umbrella



An umbrella policy will kick in after limits are breached for:

- Commercial general liability (bodily injury, property damage, personal injury, defense costs and attorney's fees, limited contractual liability)
- Business owner's liability
- Business auto liability
- Employer's liability

To avoid any of these scenarios, it's wise to carry a commercial umbrella policy, which will essentially pick up where your primary insurance leaves off – or runs out.

All of your policies have limits. Once those limits have been breached, the other party can sue and go after your firm's assets. Breaching those limits is getting easier due to the increasing prices of vehicles as well as health care costs, should the other party suffer physical injuries.

An umbrella policy will also cover you for liability for which there is no primary insurance, or when a primary policy includes an exclusion that the umbrella policy doesn't.

Most umbrella insurers require you to purchase primary insurance coverage before selling you an umbrella policy. For example, general liability insurance, auto liability in-

urance, workers' compensation or employers liability insurance.

Umbrella policy limits may range from \$1 million to \$10 million and exclusions will vary among different insurers.

### Above the umbrella

For firms that have potentially higher liabilities, an excess liability policy can be secured that kicks in after the umbrella policy is breached.

This coverage provides extra liability limits over an umbrella policy, and typically follows the terms of the first underlying insurance policy.

Higher limits may be necessary for businesses with high loss potential, high profile, sizable sales, numerous assets, large auto fleets, worldwide presence, and/or significant public exposure. ❖



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 2015 all rights reserved.