HEFFERNAN INSURANCE BROKERS
Because You're Different

News You Can Use

Nov. 2015 Volume 4, Issue 1

WORKERS' COMPENSATION

Drug Testing of Injured Workers Skyrockets

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

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

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

The main reason is to detect abuse of addictive prescription pain meds known as opioids, and similar drugs. Opioids can 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 more 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.

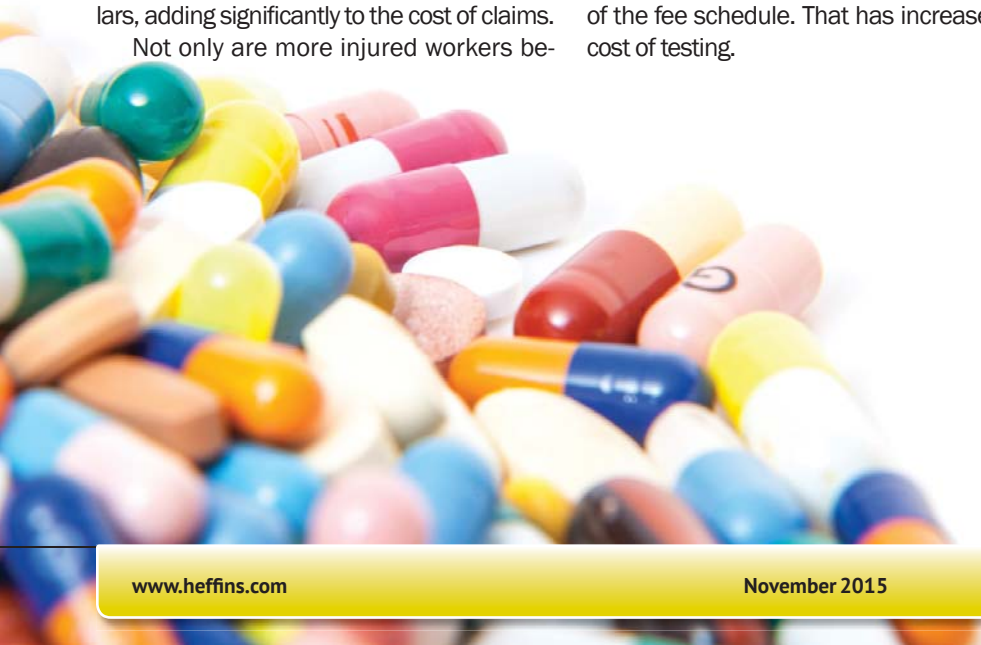
Doctors need to identify patients abusing drugs to avoid providing them opioids and change the treatment required for them.

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. ❖



HEFFERNAN INSURANCE BROKERS

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
Orange County
New York

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

SECURITY CONCERNS

Mobile Threat Booms: Revisit Your BYOD Policies

WITH 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 companies' 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 polices:

- **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. ❖

HEALTH PLAN AUDITS

Probe Triggers and What Auditors Look for

AS THE Affordable Care Act takes hold further, government agencies are stepping up their audits of health plans across the country.

With many employers still unclear over exactly what they need to do to fully comply with all the sections of the ACA – from providing affordable insurance to reporting on their plans – the risk is great that you may be found not in compliance at least in some area.

There are three government entities that are responsible for auditing employer health plans, and they all have different areas of responsibility.

While one entity may audit an employer, all three are now cooperating with each other and sharing information. This has significant implications for employers.

Health benefits attorneys have noted that if an auditor finds an infraction that may not be part of their agency's auditing purview, they are passing the information on to other agencies.

For the purposes of this article we will be focused on the audits that are most likely to happen, and the main triggers for these audits.

DOL audits

- **Adult children** – The ACA requires group health plans to allow enrollees to keep grown children up the age of 26 on their family coverage. The Department of Labor requires a sample of the written notice describing enrollment rights for dependent children up to age 26 who have used the plan since September 23, 2010.
- **Rescission of coverage** – If a plan has been rescinded, the DOL requires a list of all affected enrollees and a copy of the written notice 30 days in advance of each rescission.
- **Grandfather status** – Employers that are retaining grandfathered plan status must provide documentation to substantiate that status, as well as a copy of the required annual notice distributed to participants advising of the plan's grandfather protections.

It's been reported that the DOL seems to have a general disregard for grandfathered plans and may give them extra scrutiny.

- **Waiting periods** – The ACA bars employers from requiring that new hires wait more than 90 days before they are offered health insurance. Expect an audit if you are not complying with these rules.

IRS audits

- **ACA reporting** – Employers are required to self-report their efforts to offer full-time employees compliant health insurance coverage. Failure to comply with the reporting requirement may result in penalties of $100 per incident, up to $1.5 million. Employers need to make sure that they comply with these reporting requirements.

Also, there are assessments exceeding $3,000 a year per worker if the coverage you are offering your employees is not affordable. Even if you are offering what you think is affordable coverage to all of your workers, because people are paid different wages, coverage may not be affordable to those who are paid the least.

- **Not tracking hours** – The standard for discerning if an individual is a full-time employee is that they work more than 130 hours a month. If you have a number of part-time employees whose hours vary month to month, it's going to be difficult to gauge who is a full-timer.

The IRS lets firms use a few different methods for tracking hours for the purposes of the ACA, but the variable-hour tracking method is the most complex and may invite additional IRS scrutiny.

The takeaway

The key is preparation for any employer that wants to pass an audit without incurring penalties.

We can work with you to ensure that you have the proper supporting documentation in place in case you are contacted for an audit. ❖

Auditing Agencies

Department of Labor

- ACA
- Employee Retirement Security Act
- Health Insurance Portability and Accountability Act

Department of Health and Human Services

- Summary of Benefit Coverage compliance
- HIPPA privacy, security and breach notification rules
- Medicare secondary payer

Internal Revenue Service

- ACA (also including reporting)
- Misclassification of workers as independent contractors
- COBRA issues
- Tax issues concerning employee benefits

RISK MANAGEMENT

Flood Insurance Can Save Your Firm from Ruin

WITH 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 make this decision. ❖

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

CALL US TODAY! 877-731-7905