HEFFERNAN INSURANCE BROKERS
Because You're Different

News You Can Use

July 2016 Volume 4, Issue 9

WORKERS' COMPENSATION

Fraud Epidemic among Providers Booms in California

IN WHAT could be just the tip of a fraud iceberg, prosecutors have filed charges against nearly 100 medical providers in Southern California in cases involving more than 100,000 injured workers.

The cases include "cappers," who are typically paid about $100 per patient to recruit injured workers, to doctors and medical "mills" that provide the same treatment to every claimant they see, regardless of their injuries.

One scam includes referring workers to unnecessary care to justify billing for medical-legal reports that cost about $1,000 each.

These cases should be a wake-up call for employers, who need to look for the warning signs that one of their injured workers has been swept up in a scam that can negatively affect their X-Mods and the premiums that they will pay in the future.

What you can do

As an employer, it's difficult since you probably won't be seeing the bills as they come in.

Some experts recommend educating workers about the benefits of staying in the insurance company's network of treating physicians.

They should be educated in the dangers of succumbing to advice to go to a certain doctor while they are already receiving treatment from a physician designated by the insurer.

Also, they should be told that if they feel that a certain procedure is obviously unrelated to their condition, they should speak up and request a second opinion. If they are faced with this kind of situation, they should inform your H.R. administrator or whoever you have designated in your office to oversee your workers' comp.

They can also make their concerns known to the claims adjuster.

The only way to put a dent in this type of fraud is through employee cooperation. You should stress to your staff the importance of being aware so they are not sent for unnecessary treatment that could put their health at risk, particularly if treatment includes shockwave therapy or spinal surgery. ❖

THE SCAMS

The scams being perpetrated typically involve bribes and kickbacks being paid to doctors who refer injured workers to other doctors or medical providers, which in turn perform unnecessary, expensive procedures or dispense expensive "medicines."

$100,000 a month in bribes

Dr. Philip Sobol pleaded guilty to taking $100,000 a month in bribes to send patents to doctors who performed invasive spinal surgeries.

Questionable treatment

One worker testified that doctors referred her for questionable shockwave therapy and acupuncture to treat an injured knee. Providers billed the insurer $95,000 in medical fees.

Expensive pain cream

Prosecutors filed charges against the owner of Landmark Medical Management, accusing him of paying kickbacks so his firm could supply expensive medicated pain creams to injured workers. The firm billed insurers more than $100 million.

Excessive procedures

Dr. Ronald Grusd was indicted for bribing a doctor to send injured workers to his imaging treatment centers for MRIs, shockwave therapy and nerve tests, which were deemed questionable considering the injuries of the workers.

Contact Us

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

CYBER ATTACKS

Despite Threat, Few Firms Train Staff in Security

EVEN THE most up-to-date firewall and virus protection will not protect you against the biggest threat to your organization's cyber security – your employees themselves.

Despite this only 45% of companies train their workers in how to prevent breaches, according to a new report released by the Ponemon Institute, even though 55% of organizations surveyed said they believe they had had a security breach caused by a malicious or negligent employee. And, 66% of respondents said employees are the weakest link in their efforts to create a strong security environment.

How Employers Are Training

- 49% said training included phishing and social engineering attacks.
- 36% said training included mobile device security.
- 29% said the course included how to use cloud services securely.
- 67% said their organizations did not provide incentives to employees for being proactive in protecting sensitive information or reporting potential cyber threats.

With the obvious disconnect between employee training and the very real constant threat to any organization with a database, many companies are not doing enough on the personnel side to reduce the threat of cyber attacks, like hacking, malware and other malicious code.

Experian Data Breach Resolution, which sponsored Ponemon's "Managing Insider Risk through Training & Culture" report, had the following recommendations of what employee training should cover to protect a business from cyber attack.

Gamify training to make learning about potential security threats fun. Interactive games that illustrate threats for employees can make the educational experience enjoyable and the content easier to retain. There are new training technologies that simulate real phishing e-mails and provide simple ways to report potentially fraudulent messages.

Experian also recommends that employers provide incentives to employees for being proactive in protecting sensitive information or reporting potential issues. This could include a cash reward or gift card at a local coffee shop.

Another approach to changing behavior is to have clear consequences for negligent behavior, such as inclusion in the next performance review or a mandatory one-on-one meeting with a superior.

In addition to training, you should send regular messages to employees about security and privacy practices.

If you have had a data breach, you should require your staff to retake cyber security training. A breach provides the opportunity for you to train your staff about the importance of carefully handling sensitive and confidential information.

Insured protection

While you may have strong firewalls and a solid employee training program, if you do incur a breach, the fallout can cost you. A cyber liability insurance policy can pay for recovery costs, the cost of litigation and fines and notification costs you may incur.

Call us to see if a cyber liability insurance policy is right for your organization. The chances are extremely high that at some point, your systems will be breached. ❖

Training Emphasis

Basic courses should typically cover:

- Protecting paper documents
- Securing protected data
- Password security
- Privacy laws and regulations
- Data classification
- Safe e-mail practices

Advanced courses should typically cover:

- Phishing and social engineering
- Responding to a data loss or theft
- Mobile device security
- E-mail hygiene

WORKPLACE SAFETY

Why Your Firm Needs a Total Ban on Cell-phone Use

DISTRACTED DRIVING from smart phone use is becoming one of the leading causes of accidents in the U.S., and for the first time overall roadway deaths and injuries have started rising again despite regular advancements in car safety – a change that experts attribute to the scourge.

And as if that news is not bad enough, if one of your employees while driving for you on the job injures or kills someone while using a mobile phone, your organization could face serious liabilities. This is especially true if they were either talking on the phone without a hands-free device or using texting or some other smart phone function while behind the wheel.

But lately, juries have even been awarding large judgments in cases when a motorist was using a hands-free set while driving.

If a court were to find your driver negligent, the resulting damages could put you out of business or seriously dent your company's finances.

That's why you need to implement workplace rules to prevent distracted driving. If you have not done so, you should – and you can use the National Safety Council's cell-phone kit as a basis for those policies. ❖

Sample Policy

The NSC recommends that you have a policy that includes a total cell-phone ban on all employees while they are driving, including the use of hands-free devices. Research has shown that hands-free devices are not safer than handheld phones because the cognitive distraction still exists.

In its kit, the NSC includes a sample cell-phone policy, which reads: "Due to the increasing number of crashes resulting from the use of cell phones while driving, we are instituting a new policy. Company employees may not use cellular telephones or mobile electronic devices while operating a motor vehicle under any of the following situations, regardless of whether a hands-free device is used:

- When the employee is operating a vehicle owned, leased or rented by the company.
- When the employee is operating a personal motor vehicle in connection with company business.
- When the motor vehicle is on company property.
- When the cellular telephone or mobile electronic device is company owned or leased.
- When the employee is using the cellular telephone or mobile electronic device to conduct company business."

You can find the NSA kit at: www.nsc.org

Liability wake-up call

- A jury in Texas found a beverage company liable after one of its drivers crashed while using a hands-free device, even though the headset complied with the company's policy. **Verdict: $21 million.**
- A jury in Arkansas found a lumber distributor liable after one of its salesmen rear-ended another car while talking on a mobile phone. **Verdict: $16 million**.
- A jury in Ohio ordered a national technology communications company to pay damages after one of its drivers, while using a cell phone, crashed into another car and killed one of the occupants. **Verdict: $21.6 million.**

The facts

- The NSC model estimates 21% of crashes, or 1.2 million crashes in 2013, involved talking on handheld and hands-free cell phones.
- The model estimates an additional 6% or more crashes, or a minimum of 341,000 of crashes in 2013, involved text messaging.
- Hence, a minimum of 27% of crashes involved drivers talking and texting on cell phones, according to the model.

C-SUITE LIABILITY

Small Firms Need Directors & Officers Coverage

WHILE DIRECTORS and officers liability has been traditionally thought of as insurance for publicly traded companies, increasingly it's smaller companies that account for the largest share of exposure among top decision-makers.

A study published by the news website *Advisen* found that over the past 10 years, small businesses accounted for 70% of all D&O insurance claims. And during that time, these claims increased 300% for small businesses, compared with 200% for large companies and 150% for mid-sized operations.

Although privately held businesses don't risk exposure to securities class-action suits, a business doesn't have to have shareholders in order for its directors and/or officers to be personally sued.

Low-priced policies for small firms

Many insurance companies now offer small business executive liability coverage starting at $1,500 per year to protect directors and officers.

D&O liability insurance protects corporate directors and officers in the event they are personally sued – often in addition to the company being sued – by investors, employees, vendors, competitors and customers, among other parties.

The insurance protects directors and officers by covering legal fees, settlements and other costs; in addition, the coverage sometimes can extend to protect the company if it is named in a suit, as well.

Also, some new directors or officers may demand that you purchase D&O insurance as a condition of employment or serving, since they will not want to put their personal assets at risk. Outside investors may also demand that you purchase a policy before agreeing to fund your company. ❖

When to consider D&O insurance

- If your company has relationships with vendors and customers that could in some way leave your directors or officers exposed.
- If you intend to seek venture capital funding or attract other investors.
- You have officers or directors who could be targeted by litigants over their management of company affairs.

Coverage examples

Your directors and officers may face exposure to lawsuits and regulatory actions that could seriously dent your company's finances. Consider the following risks that a D&O policy would cover:

Breach of fiduciary duty – Investors sue a company alleging that some of its officers had personal connections to a third-party contractor the company hired to do some work. They accuse other officers and directors of breaching their duty of care in undertaking the project without properly investigating the qualifications of the contractor.

Failure to comply with workplace laws – An employee is terminated and then sues the directors and officers and the company for wrongful termination based on gender discrimination.

Theft of intellectual property – You hire a new vice president and his former employer sues him and your company, accusing him of stealing certain corporate licenses to market proprietary software, creating unfair competition and trademark infringement.

Misrepresentation – A company asks a supplier to build up its inventory because it expects an uptick in business. The supplier complies and then the company switches suppliers. The original supplier sues, alleging damages based on the promise of more business and subsequent failure to provide that business.

Want to know more? Call Us! 877.731.7905