Leaderschoice
INSURANCE SERVICES

Leaders News Alert

February 2014, Volume 4, Issue 2

Affordable Care Act

Enrollee Rush, Back-end Glitches Cause Delays for Health Plans

INSURANCE COMPANIES are scrambling to catch up with the onslaught of new policies sold through public insurance exchanges set up under the Affordable Care Act.

As of the middle of January, the *Los Angeles Times* reported that many policyholders had yet to receive their health ID cards, which they need to prove coverage for sometimes vital medical procedures.

These delays are the result of the Obama administration issuing orders to postpone the deadline for purchasing coverage under the ACA, as well as glitches in the *HealthCare.gov* exchange through which individuals could purchase coverage from a menu of insurance companies and plans.

The sign-up period for the individuals purchasing policies through the health insurance exchange started on Oct. 1, but glitches in the website resulted in few people being able to secure coverage.

In the first two months, only 364,500 people had signed up for coverage on the exchanges well short of expectations due to website problems. After fixes to the front-end of the site, the one invidiuals use to select coverage, enrollment surged in December by 1.8 million people.

Due to the slow uptake, the administration announced that the deadline for signing up for coverage for 2014 would be pushed to Dec. 23 from Dec. 15.

The combination of the problems with the online marketplace and the enrollment deadline postponement created an unexpected bottleneck of applications in late December. Adding to the tumult was the flood of policy cancellations for millions of Americans in November.

Enrollment file issues

Insurers also say both federal and state exchange websites have been sending erroneous enrollment files to them, or data that is either delayed or lost completely.

Under the exchange structure, enrollment information is sent from the federal government to insurers. In some cases, the information transferred has been delayed – or it's not been transferred at all.

And in fact as late as mid-January, an administration official told Congress that the "back end" (the part that communicates and sends payments to the insurance companies) of *HealthCare.gov* was still being built – and he didn't forecast a completion date.

The automated system that is supposed send payments to insurance companies isn't finished.

The payment system will transfer directly to insurers the federal subsidies some consumers get to help pay for their premiums. The official told the committe that as Jan. 16, about 30% of the federal health insurance

See 'Payments' on page 2

CORNER OF LOST AND CONFUSED: *Due to the onslaught of new enrollees, health insurers are struggling to keep up with issuing plan materials.*

Time to Post 300A Forms

FIRMS WITH 10 or more employees must maintain a Cal/OSHA 300 Log of Work-Related Injuries and Illnesses during the year and record a summary on the 300A, which must be posted no later than Feb. 1.

Make sure to provide the mandatory information, as the forms can be admissible in court proceedings.

You must complete the summary page, even if no work-related injuries or illnesses occurred last year.

The form must be posted in a common area of the workplace, from Feb. 1 to April 30. You must keep the records for five years following the calendar year covered by them, and if the you sell the business, you must transfer the records to the new owner. ❖

CONTACT US

Leaderschoice
INSURANCE SERVICES

2520 Venture Oaks Way, Suite 310
Sacramento, CA 95833

Phone: 866.211.2123
Fax: 866.913.7036
www.leaderschoiceins.com

License No. 0G80276

If you would like to receive this newsletter electronically, e-mail us at: info@leaderschoiceins.com.

Workers' Comp

Pay Attention to Policy Milestones to Reduce Costs

ONCE THEY'VE paid their annual premium, many employers pay scant attention to their workers' comp policy until the renewal date starts closing in. Unfortunately, that's not the best time to attempt to control costs.

Because workers' comp is one of the most loss-sensitive insurance policies, and as claims can sometimes be paid out for decades, it's incumbent on you to proactively manage claims. One way to do that is through a quarterly claims review process, the timing of which is in line with the calculation of your company's Experience Modification Factor (X-Mod), which is the one factor you can control to reduce premiums.

It's important to review loss runs and assess all open claims three months into the new policy year, because the critical number crunching for calculating the X-Mod takes place six months after the policy anniversary date. This gives you three months to reduce or close claims that will affect the X-Mod calculation.

X-Mod
Check
3 Months:
Loss Runs
6 Months:
Unit Stat

Policies that renewed on Jan. 1, 2014 used the losses from policies that were effective in 2010; 2011; and 2012. In other words, it looks at the claims from four years ago to one year prior. It will not include the most recent year's claims payouts, as they are still too fresh.

This is when it's time to focus on trying to close claims and reducing reserves on existing claims.

The top priority is getting the injured employees back to full or modified duty. If that isn't possible and return to work appears unlikely, then consideration should be given to settling the claim.

Six months after policy inception is the most important day of the workers' comp year, because this is when the insurance company sends loss information to the rating bureau to be used in the calculation of your X-Mod. This is known as the "valuation date," or sometimes, the "unit stat" date.

This information includes not only the money that the insurance company has spent on claims, but also what it expects to spend (the reserves). In effect, your insurer takes a snapshot of your loss information and it is absolutely critical that these numbers be correct.

With few exceptions, once the bureau has the numbers, they are set in stone.

Unfortunately, the numbers are often inaccurate because gauging claims costs is not an exact science. Also, errors are rampart in the system and, once an insurer sets reserves for a claim, it is hard to get them reduced until after the claim closes.

The window of opportunity is short and the process of correcting mistakes can take time, which is another reason for the comprehensive review three months after the policy's inception.

Put reserves in focus

Pay close attention to reserves. The reserves represent what the insurance company thinks the ultimate cost of the claim will be. It is not a guess, but it is more of an art than a science. Its accuracy depends on the precision of the adjuster in evaluating the employee's medical condition, anticipated time away from work, cost of medical care and other relevant costs.

Yet, the cost projections get counted exactly the same as the dollars paid out, so if the reserve is set too high, you will pay too much.

Although the X-Mod is set at the sixth-month mark, it is a good idea to continue the quarterly review process at nine months. Throughout the year, proactive management of all open claims will ensure that you don't get any surprises at renewal. ❖

Continued from page 1

Many New Enrollees Late in Making First Payments

marketplace was still being developed.

All of these problems have resulted in insurers not sending out coverage ID cards and plan materials in a timely fashion. And in some cases, even though some individuals had received ID cards, they'd yet to pay for coverage, which left them in a bind when at the doctor's office or at a pharmacy picking up drugs.

WellPoint, the nation's second-largest health insurer, told the *New York Times* that it had responded to more than 1 million customer calls over two days in early January, equal to the amount it typically receives over an entire month. It has more than 1,000 employees answering calls.Recent government changes to the law's implementation and deadlines "are impacting the timeline for us to process customer applications, issue billing statements, process payment and issue coverage ID cards," WellPoint spokeswoman Kristin Binns told the *Times*.

"We greatly appreciate patience during this transitional time and apologize for any inconvenience they may have experienced," she added.

Another issue facing the insurers is late payments. Even though many of them had extended the payment deadline to Jan. 15 because of the later enrollment deadline, by the deadline many insurers were struggling to collect.

"It's been pulling teeth," Shaun Greene, chief operating officer of Utah-based Arches Health Plan, told the *Wall Street Journal* in a Jan. 14 article.

At that time, Arches had collected about 60% of premiums for people who signed up for coverage that took effect Jan. 1. ❖

Risk Management

Top Threats Facing Businesses This Year

BUSINESS INTERRUPTION and natural disasters will be the biggest threats for companies in 2014, according to the "Allianz Risk Barometer".

The top 10 threats also include, for the first time, cyber crime and reputational loss. Other significant concerns for risk managers and corporate executives surveyed around the world include fires and explosions, and changes in regulations and laws.

The report is a good starting point for companies that want to minimize their risk via proper risk management and planning, as well as through insurance to provide coverage should problems arise.

The report highlights just how complex the risks to business have become and that companies need to establish strong internal controls and regularly gauge the environment for these threats that can, in some cases, cripple a business if it's unprepared.

Many of the top 10 threats are interrelated. For example, reputational risk grows should a cyber attack result in harm to customers, and supply chains can be disrupted should an IT failure occur due to a hacking attack.

This article looks at the main risks and the ones that are increasingly on corporate executives' radars.

Supply chain disruption and business interruption

Allianz Global Corporate & Specialty estimates that business interruption and supply chain-related losses account for 50-70% of insured property catastrophe losses – as much as $26 billion a year.

Interruptions can be caused by a number of events such as natural disasters, political and societal instability, transportation disruptions and IT outages, among others. Indeed, now more than ever it's important that you work closely with your most-used suppliers to devise plans for dealing with supply chain disruptions.

When a disruption occurs, you need to have mitigation plans in place to prevent loss of market share to better prepared or less affected competitors.

Some key things to consider in regards to supply chain disruption:

- To reduce their supply chain risk, some companies operate with greater inventory than you typically see in lean manufacturing. You may also want to consider giving a small amount of your business to another supplier, so that you have a relationship with it in case your main source has a supply chain problem.
- Have plans for keeping business going in case of disruption.
- **Talk to us about business interruption insurance coverage.**

Natural catastrophes

There is no doubt that the weather has become more volatile in recent years. Allianz identifies four key steps businesses can implement now to be better prepared for future extreme weather events:

- Update and test emergency preparedness plans;
- Review business contingency plans;
- Understand your insurance policy; and
- Know what to prepare for (which will vary depending on where your business is located).

Depending on the disaster, your property policy may or may not cover the damage. Threats such as flooding and earthquake are typically not covered and require added coverage. We can help you.

Cyber threat and reputational risk

According to Allianz, the most heightened risk awareness in 2014 is around cyber and loss of reputation issues, with risk managers around the world increasingly on red alert about the threat such fast-evolving, high-tech perils pose.

Besides customer information, a cyber breach can also expose corporate secrets, vital information on suppliers – and your employees' data, too. Worse, studies have found that hackers are increasingly turning their attention to small and mid-sized businesses, which typically have lower defenses than their corporate counterparts.

Amid rising cyber criminality, IT security is not enough. You need strong policies and procedures in place as well as cyber liability coverage. Call us for details. ❖

The Top 10 Risks as Ranked By Executives

1. Business interruption, supply chain
2. Natural catastrophes
3. Fire/explosion
4. Loss of reputation, brand value
5. Cyber crime, IT failure, espionage
6. Intensified competition
7. Quality deficiencies, serial defects
8. Environmental changes
9. Changes in laws and regulations
10. Market stagnation or decline

SOURCE: Allianz Risk Barometer

Cyber Threats

Five Ways to Boost Your Social Media Security

AS MORE companies take to social media to reach out to their clients and attract new ones, the threats grow.

Accounts are hacked, changed or used to disseminate messages that vilify the company that has been hacked. Sometimes profiles and follower lists have also disappeared. And a company whose Facebook or Twitter account is hacked can expect some damage to its brand.

However, while the attacks are malicious, they are avoidable. Most of the time when a social media account is hacked, it is the result of a simple scam and lack of caution by the individual operating the account. Sometimes the attack is made possible by employees opening suspicious e-mails or websites, or passwords being shared by e-mail.

The company Hootsuite, a social media management firm, has created a list of five solutions to the most common security challenges related to social media. Here it is:

- **Training your staff** – There are structured social media training programs and kits online, and through them employees can learn the best practices for utilizing social networks for the benefit of your company while maintaining secure control.

You can teach employees how to spot a malicious link, which is the most common way to hoax or phish in order to compromise social media accounts. Be especially wary of links that ask for usernames or passwords, as they are hoping you'll enter your preferred IDs.

- **Centralize your social media channels** – Audit all of your company's social media accounts, taking note of who manages them and who has access to them.

There are social media management systems that allow you to draft messages and publish them to different social media platforms from one interface. They also allow those responsible for keeping your site up to date to monitor all social media messaging and activity from the same place.

These systems often have built-in malware and spam tools that can notify users when they click a suspect link.

- **Protect passwords** – Shared social media accounts inevitably mean shared passwords, which means they need to be protected so they don't fall into the wrong hands. The first step in password protection is actually taking the time to build a strong and complex password with a mix of upper- and lower-case letters as well as digits.

Employees should be certain to never store the password on shared computers, within e-mails or on mobile devices that could ever be stolen or lost.

A good strategy is to use a password management tool like LastPass or KeePass that can create as well as share passwords without making them physically visible to other members of the team.

- **Start a messaging approval system** – There is a very simple way to reduce the likelihood of a mis-Tweet from ever getting sent out from a corporate account: a two-step approval process. Social media management systems offer teams the ability to put in place an approval process for all social messaging.

This means that two sets of eyes will see every Tweet and Facebook post before they become public, drastically reducing the likelihood of an accidental or purposefully harmful mis-Tweet from getting through.

- **Prepare for problems** – Every enterprise should have a specific crisis plan in place in case something goes wrong. This means employees should be trained very specifically on how to respond quickly and effectively during a crisis.

Plans should be simple and flexible, since crises tend to be unpredictable.

Social media happens in real-time, which means that a company needs to respond to a situation in real-time as well. Social media management tools can serve as a command center, allowing you to oversee all communications at once.

These tools can alert you to a potentially harmful situation or odd activity on your accounts. ❖

Produced by Risk Media Solutions on behalf of Leaders Choice Insurance Services. 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.