August 2013 Volume 1, Issue 12

Curry Insurance Agency

HEALTH REFORM

Employer Mandate Delayed – Now What?

AS YOU ARE probably aware, the IRS announced on July 9 that the Affordable Care Act mandate that employers of 50 or more full-time workers provide their staff with health coverage had been delayed for a year until 2015.

And while many employers breathed a sigh of relief at the news, that does not mean they should put up their feet and forget about it all until sometime next year.

That's because there are still a number of requirements and deadlines that employers and their health plans must comply with, starting Oct. 1 of this year.

Further, we advise that you continue planning and prepare for the eventual start of the employer mandate for a number of reasons.

Even though IRS reporting requirements have been delayed along with the employer mandate, the IRS is encouraging employers to voluntarily comply in 2014 with its information reporting requirements, which have yet to be released.

By trial-complying early you will be able to test your systems, which should make it easier for you when the reporting requirement becomes mandatory in 2015.

What are the reporting requirements?

Information to be provided includes:

- The name and Employer Identification Number ("EIN") of the employer.
- If the employer offers full-time employees the opportunity to enroll:
  - The duration of any waiting period,
  - Months during the calendar year when coverage under the plan was available,
  - The monthly premium for the lowest-cost option in each enrollment category under the plan,
  - The employer's share of the total costs of benefits provided under the plan,
- The number of full-time employees for each month during the calendar year, and
- For each full-time employee, the name, address, Tax Identification Number and the months during which the employee (and any dependents) were covered under the plan.

Although no penalties will be assessed for 2014, employers should evaluate what steps are still needed to offer affordable, minimum coverage to all full-time employees if they want to avoid penalties in 2015.

And if you have a plan that operates on anything but a calendar year (meaning it does not incept on Jan. 1), you need to decide if you want to implement any needed changes at the beginning of the plan year that begins in 2014 and runs into 2015, or delay any changes until Jan. 1, 2015 and offer newly eligible employees a mid-plan-year enrollment opportunity.

Requirements that take effect Jan. 1

A number of ACA insurance reforms and benefits requirements that apply to group health plans beginning in 2014 still apply. This means that for plan years beginning on and after Jan. 1, 2014, all group health plans must:

- Eliminate all pre-existing condition exclusions (regardless of age);
- Eliminate annual limits on the dollar amount of essential health benefits; and
- Eliminate waiting periods of longer than 90 days for new hires.

In addition, for plan years beginning on or after Jan. 1, 2014, non-grandfathered group

See 'Squander' on page 2

NO TIME TO RELAX: *Just because you have more time, don't put your feet up for the next year.*

CONTACT US

If you have any question 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

WORKERS' COMP

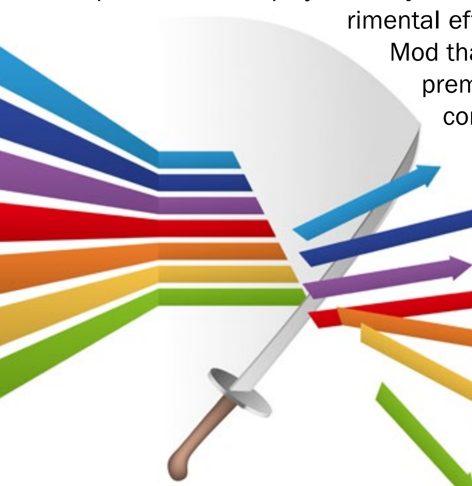
Push Is on to Reduce Single Claim's Effect on X-Mod

AFTER MANY smaller employers felt the stinging effects of changes to the way X-Mods are calculated starting with the 2013 policy year, the state's rating agency is looking at ways to temper consequences for employers that get hit with a single claim.

Currently, if a worker for a small employer suffers a workplace injury, the firm's X-Mod can climb by more than 50 points under rules prescribed by the California experience rating plan. But, the Workers' Compensation Insurance Rating Bureau is mulling a proposal that would limit that increase to 25 points, although employer members of its governing board want a maximum of 15 points.

The idea would be to establish rules that ensure that the amount of an increase in the employer's premium is relative to the cost of the claim that triggered the X-Mod change.

The reason for the Bureau considering the change is complaints from employers that just one claim can have such a detrimental effect on a small employer's X-Mod that it results in a large enough premium increase to threaten the company's survival.



The sector that's been most vocal about pressing for the rule change is the construction industry. In many cases, terms of reference for new projects will mandate that those bidding for a job have a X-Mod that is no greater than a certain level, say 90, 100 or 125. Under current regs, if a claims-free contractor has an X-Mod of 80, one average-sized claim of $30,000 can push their X-Mod up beyond 130 points, which disqualifies them from bidding on most jobs.

The Bureau's proposal of a 25-point swing limit would keep these employers on the lists with an eligibility limit of a 125 X-Mod, but employer representatives say that a 25-point maximum is still draconian and are pushing for a maximum swing of 15, as they would still be unable to bid on one that requires a 100 X-Mod.

Disproportionate effect

Another issue is the effect of smaller claims on an X-Mod under the so-called primary and excess value of claims.

In the experience rating process, each loss is divided into a primary and an excess portion. Currently, the first $7,500 of every loss in California is allocated as a primary loss, with everything over and above considered an excess loss. For example, a $3,000 loss has no excess value.

On the other hand, a loss of $15,000 would have $7,500 in primary losses as well as $7,500 in excess losses.

Primary losses are used as an indicator of frequency, and are counted in full as part of the X-Mod calculation. But, excess losses receive partial weight in the calculation. This means that primary losses affect the X-Mod more than excess losses do.

And that's why – according to research by UC Berkeley's Survey Research Center – a $4,000 claim would cause the small employer to pay out an extra $12,000 to $16,000 in workers' comp premiums over the next three years.

The Bureau is also looking at ways to minimize the effects of claims that fall under the $7,500 split, as one claim can disproportionately affect a small employer's X-Mod. ❖

Continued from page 2

Don't Squander the Added Time by Failing to Plan

In addition, for plan years beginning on or after Jan. 1, 2014, non-grandfathered group health plans must:

- Limit cost-sharing provisions as follows:
  - Insured plans in the small-group market must limit any annual deductibles to $2,000/individual ($4,000/family);
  - All group plans must limit in-network out-of-pocket maximums to $6,350/individual ($12,700/family);
- Not discriminate against a health care provider acting within the scope of that provider's license or certification; and
- Provide certain, nondiscriminatory benefits for individuals who participate in clinical trials.

State insurance exchanges notification requirement

With state health insurance exchanges still scheduled to begin enrolling individuals for coverage that take will take effect Jan. 1, 2014, most employers will still be required to send out notice of exchanges to their employees before Oct. 1.

These notices must be sent to current employees by Oct. 1,. After that date, employers will be required to send the notice to new employees within 14 days of their start date.

The Department of Labor has issued a model notice for employers that currently offer coverage to their employees, which is available here:

http://www.dol.gov/ebsa/pdf/FLSAwithplans.pdf

There is also a model notice for employers that do not offer their employees coverage:

http://www.dol.gov/ebsa/pdf/FLSAwithoutplans.pdf

And for those employers that don't offer coverage for 2014, but plan to do so for 2015, they may need to send an updated notice of exchanges to employees in 2014 to reflect their status change. ❖

RISK MANAGEMENT

Top 10 Reasons You Need a Cyber Liability Policy

WITH REPORTS of cyber criminals increasingly focusing on smaller companies for targeted attacks, now more than ever employers that store sensitive data need to consider how they protect their information systems, as well as other steps in case they are hit.

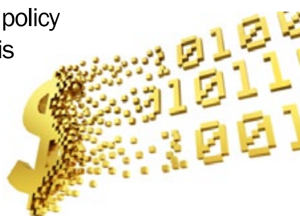
And while you can install firewalls and take other precautionary measures, should an attack occur, you will be left facing untold costs and possible fines and lawsuits by those whose data may have been exposed. One way to protect your company is by securing a cyber liability policy.

But what does a cyber policy cover, and why should you get one? You may think an attack may never target your firm, but if it does and you are without insurance coverage, you may be sorry you didn't act.

The following are the top 10 reasons for buying a cyber liability policy:

1. Data is a valuable asset

Your data is almost certainly worth many times more than the physical equipment that it is stored upon. Yet most business owners do not realize that a standard property policy would not respond in the event that this data is damaged or destroyed. A cyber policy can provide comprehensive cover for data restoration and rectification in the event of a loss, no matter how it was caused and up to the full policy limits.



2. Systems downtime is not covered by business interruption policy

If a cyber attack, computer virus or malicious employee brings down electronic point of sales software or other important electronic functions, a traditional business interruption policy would not respond. Cyber insurance can provide cover for loss of profits associated with a systems outage that is caused by a computer virus or denial-of-service attack.

3. Cyber crime is fastest-growing crime

Thanks to the world wide web, your business is now exposed to the world's criminals and is vulnerable to attack at any time of the day or night. Phishing scams, identity theft and telephone hacking are all crimes that traditional insurance policies do not address. Cyber insurance can provide comprehensive crime cover for a wide range of electronic perils that threaten your financial resources.

4. Your company can be held liable if it loses third-party information

Non-disclosure agreements and commercial contracts often contain warranties and indemnities in relation to the security of data that can trigger expensive damages claims in the event of a breach. Besides, consumers are also seeking legal redress after businesses lose their data. You can also be subject to fines by state authorities for not acting quickly and notifying clients whose data may have been breached.

5. Retailers face severe penalties if they lose customer credit card data

Global credit card crime is worth over $7.5 billion, and increasingly this risk is being transferred to the retailers that lose the data. Under merchant service agreements, compromised retailers can be held liable for forensic investigation costs, credit card reissuance costs and the actual fraud conducted on stolen cards. These losses can run into hundreds of thousands of dollars for even a small retailer. Cyber insurance can help protect against all of these costs.

6. Complying with breach notification laws costs time and money

Breach notification laws generally require businesses that lose personal data to notify individuals that were potentially affected. Customers who have had their data compromised expect openness and transparency from the businesses they entrusted it with. Cyber policies can cover costs associated with providing a breach notice, even if it is not legally required.

7. Your reputation is your number one asset, so why not insure it?

Although there are certain reputational risks that can't be insured, you can insure your reputation in the event of a security breach. When your systems have been compromised, you run a risk of losing the trust of your loyal customers, which can harm your business far more than the immediate financial loss. Cyber insurance can not only help pay for the costs of engaging a PR firm to help restore this, but also for the loss of future sales that arise as a direct result of customers switching to your competitors.

8. Social media claims on the rise

A lack control over what employees say on behalf of the company on social media can be a liability for businesses. Cyber insurance can help cover claims arising from leaked information, defamatory statements or copyright infringement.

See 'Cyber' on page 4

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 2013 all rights reserved.

WORKERS' COMP

New Dividend Rules in the Making in California

THE CALIFORNIA Department of Insurance is mulling changes to the state's workers' comp dividend laws that should benefit employers.

One of the key changes that the department has proposed in draft regulations circulated in May 2013 is that it would be illegal for insurers to base any dividends to policyholders contingent upon them renewing their policy with the incumbent carrier.

This is likely in response to press reports that one carrier in California was basing dividend payments in part on the policyholder renewing their policy, in contravention of state insurance regulations. It was later warned that the practice was in contravention of those regs.

Dividends are typically paid to employers who manage to have no or few claims and that have low X-Mods. They are often based also on how profitable their policy has been to the insurance company.

Dividends are supposed to be an incentive for employers to keep their workplaces safe. Payment of dividends to workers' comp policyholders is a very common method used to adjust pricing of a policy after it expires.

Some carriers pay dividends, but many do not, prefering to perhaps provide a lower rate on the front end.

The draft rules would also require insurance companies to issue to policyholders that do not receive dividends a notice stating the reason or reasons that they were not paid a dividend.

Also of interest to smaller employers, the draft regs would jettison the current $10,000 in annual premium trigger for issuing policyholder dividend statements.

Currently, the regulations require carriers to issue the statements on policies generating $10,000 or more in annual premium, but issuing the statement on lower-valued policies is optional.

And, like stock returns, under existing regulations insurance companies cannot promise that dividends will be paid. The draft regulations go a step further by barring insurance companies from telling or promising either directly or through a broker what their dividend will be.

The proposed regulations have been sent out for comment and, after the Insurance Department reviews stakeholder input, it will release permanent regulations later this year. ❖

Typical Requirements for Dividend Policies

TYPICAL ELIGIBILITY requirements for participation in one of these plans will include:

- An employer's earned premium must be at some specific minimum level. It's common to see a minimum premium of $10,000 being required for participation. However, you may find some companies that allow lower minimums while others have higher minimum requirements.
- A minimum acceptable loss ratio is required. Below 50% is typical. This is total claims paid, including reserves, divided by earned premium.
- Your policy must remain in force for the full policy period.
- All premium must be current and paid before the dividend is due.

Continued from page 3

Cyber Liability Policy a Smart Choice as Threats Mount

9. Portable device loss or theft

A laptop left on a train, an iPad stolen in a restaurant, or a USB stick going missing are all good examples of risks that can open your company up to data theft or stolen intellectual property.

Also, the devices themselves are being targeted, with a growing number of viruses being built just for them.

A cyber policy can cover costs associated with a data breach should a portable device be lost, stolen or fall victim to a virus.

10. Small firms increasingly targeted

While the large-scale attacks in the news often involve big companies, small companies are also at risk and often don't have the financial resources to get back on track after a cyber attack or other kind of data loss. According to the "Symantec 2013 Internet Security Threat Report," the fastest growth area for targeted attacks is on businesses with fewer than 250 employees, accounting for 31% of all attacks. A cyber liability policy can help protect smaller companies against the potentially crippling financial effects of a privacy breach or data loss. ❖