

MANAGING RISK



THE ADDIS GROUP

A Susquehanna Company

2500 RENAISSANCE BOULEVARD
KING OF PRUSSIA, PA 19406-2772
(610) 279-8550
FAX (610) 279-8543
WWW.THEADDISGROUP.COM



Addis Workplace Honored

The Addis Group has been named 17th among the 50 Best Mid-Sized Places to Work in PA for 2006. The Best Places to Work in PA list is comprised of 50 large and 50 mid-sized companies. The Addis Group is honored to be ranked among these 100 Best Places to Work in PA.

These 100 companies represent a snapshot of the diverse and thriving nature of Pennsylvania's economy – an economy that balances traditional manufacturing and service organizations with innovative technology and “new economy” startups.

BEST PLACES
to work in **PA** 2006



ALSO IN THIS ISSUE

- Pandemics
- Liability for Data Breaches
- Addis News

How the “Tax Relief and Health Care Act of 2006” Will Affect HSAs



The tax bill voted upon by Congress in late 2006 included six health savings account (HSA) provisions. The tax bill also contains a number of Medicare provisions, including one that will block the 5 percent cut in Medicare payments to doctors that was scheduled to take place January 1. It also added a 1.5 percent payment incentive for doctors who begin reporting on standard quality measures in 2007. This provision is part of a shift toward performance-related reimbursement in government health programs, as suggested by President Bush's recent executive order.

More specifically, the provisions affecting HSAs would:

- Permit taxpayers who enroll in an HSA-eligible health plan midyear to make a full-year contribution to their HSAs. Current law requires the plan to impose a full-year deductible, but only allows a prorated HSA contribution.
- Allow employees a one-time, tax-free transfer of amounts in flexible spending arrangements (FSAs) or health reimbursement arrangements (HRAs) for the purpose of funding an HSA. FSA participants with a 2½-month grace period would also be allowed to contribute to an HSA during that grace period, provided that no funds remain in the participant's FSA at the end of the plan year.
- Allow HSA contributions up to the annual statutory maximums, regardless of health plan deductible. (For 2007, deductibles are \$2,850 for single coverage and \$5,650 for family coverage; they are indexed to inflation.) Current law limits HSA contributions to the lesser of the deductible on the individual's high deductible health plan or the statutory maximum.
- Require the U.S. Treasury Department to issue cost-of-living adjusted deductible and contribution requirements earlier in the year (by June 1).
- Allow employers to make higher contributions to the HSAs of non-highly compensated

HSA—continued on Page 2

Preparing for Pandemics

The World Health Organization says a pandemic could debilitate up to 25% of the workforce at one time. How will your business survive?

The U.S. hasn't seen a major pandemic since the Hong Kong flu, which caused 35,000 deaths in the U.S. in 1968. However, in a world where air travel brings 1.6 billion people across international borders each day, a highly infectious strain of influenza could become a global problem in a very short time.

Some considerations for employers:

- ✦ The World Health Organization (WHO) estimates that pandemic may debilitate up to 25 percent of the workforce at any one time. People of working age will be hit the hardest. Unlike seasonal flus, which primarily affect the young, the old and those with weakened immune systems, in past flu pandemics, 20- to 30-year-olds suffered the highest death rates.
- ✦ Vaccines will be ineffective. As pandemics occur when new or rapidly mutating viruses spread, existing vaccine stocks will not work—and it takes six months or more to develop new vaccines.
- ✦ Public health quarantines may occur, preventing workers and customers from coming to your business premises.
- ✦ Quarantines on imports may also be imposed. Even without quarantines, worker shortages and travel restrictions might interrupt the delivery of goods and materials your business needs.

Insurance considerations

Unfortunately, there's little coverage available for pandemics. Business income policies typically pay only when insured loss or damage to covered property causes a business interruption, so your policy likely will not cover income lost due to pandemic. Nor will contingent business interruption policies cover you if a pandemic closes or slows production at a "dependent location," such as a key supplier or vendor. (Some Canadian companies are developing coverage for pandemics; how-

ever, to date no American companies offer this coverage.)

A pandemic could also affect your benefits program. Pension plans that pay death benefits could face liquidity problems if death rates increase. Businesses that self-insure employee medical benefits could drain their cash flow.

Your workers' compensation program is unlikely to face pandemic-related claims, unless you are in the healthcare industry, since workers' compensation covers only work-related illnesses.

Directors and officers of publicly traded companies could face liability claims if the company experiences pandemic-related losses and shareholders allege they did not adequately prepare. Your directors and officers liability (D&O) policy may cover this type of claim. However, the best policy is to prevent this type of claim from occurring by taking reasonable steps to prepare for a pandemic.

Action steps:

- 1 Update your emergency procedures to include what to do if pandemic causes widespread illness or quarantines.
- 2 Develop flexible sick-leave policies to encourage sick employees to stay at home and avoid spreading illness.
- 3 If you self-insure medical benefits, buy adequate stop-loss insurance.
- 4 Identify all employees whose jobs (or essential functions thereof) could be performed off-site. Develop a telecommuting program to allow these people to work at home in event of emergency. Work with IT staff to get systems in place to allow telecommuting.
- 5 If a pandemic occurs, have nonessential employees stay at home. Avoid gathering large groups and substitute telecommunications wherever possible for face-to-face contact.



- 6 Educate employees on proper sanitation to prevent the spread of disease. This includes washing hands after sneezing, coughing or using the bathroom and before and after eating, and staying home when ill. Those whose immune systems are compromised might want to wear facemasks when in public.

For more information on managing the risk of pandemic, please contact your account manager at The Addis Group. ■

HSA—continued from Page 1

employees. Existing Treasury regulations also permit higher HSA contributions to lower-wage workers, but only when HSAs are offered through cafeteria plans.

- ✦ Allow taxpayers to make a one-time distribution from an Individual Retirement Account (IRA) to fund an HSA, subject to the HSA contribution limits.

As this newsletter went to press in late December, the House and Senate were working on resolving differences in the bill; however, portions relating to HSAs were expected to remain unchanged. For more information about HSAs or setting up the high-deductible health plans (HDHPs) linked to HSAs, please contact Robert M. Enderlein of The Addis Group at (610) 945-1033. ■

Protecting Your Company from Liability for Data Breaches

Preventing a data breach costs much less than correcting it.

The Privacy Rights Clearinghouse, a consumer advocacy organization in San Diego, estimates that companies and institutions have collectively “fumbled” some 93,754,333 private records, according to a recent New York Times report. Releasing an individual’s personal identifying information can expose organizations to liability for identity theft, which occurs when others use private identifying information for criminal or fraudulent purposes.

Risk exposures include:

- ✦ **Liability.** According to PLUS, the Professional Liability Underwriting Society, the number of privacy lawsuits has increased 300 percent in the last 10 years.
- ✦ **Fines.** Many federal laws govern privacy and call for penalties when an organization fails to take appropriate steps to protect individuals’ personal identifying information.

- ✦ **Notification costs.** At time of publication, 29 states (including Pennsylvania, New Jersey and New York) had laws requiring businesses and nonprofits to notify their clients when their personal information is breached. Laws will take effect in Kansas, New Hampshire and Utah on January 1, 2007. Standards for notification vary by state—stricter standards, such as California’s, call for notification for any breach. For details on state requirements, see the State PIRGs (Public Research Interest Groups) site at www.pirg.org/consumer/credit/statelaws.htm.

What does notifying customers cost? A survey by the Ponemon Institute found that each lost record costs companies an average of \$140, for a total of \$5 million in direct costs per incident.

- ✦ **Public relations costs.** A breach of customer information can also damage an organization’s reputation. Another study by the Ponemon Institute found that, of the 23 million U.S. adults who have been notified of a breach of their personal data, approximately 20 percent terminated their accounts and another 40 percent were considering it. Adverse publicity from the breach will likely impact sales as well.

How do you prevent data breaches?

To protect your business from liability for data breaches, familiarize yourself with any federal and state privacy laws. Different laws apply to different types of organizations, however, the Fair and Accurate Credit

Transactions Act applies to any business or individual who uses consumer information for business purposes. It requires them to dispose of this information properly to prevent unauthorized access.

Action steps you can take to minimize your exposures include:

- ✦ Ensure your IT department uses the latest technology to secure data and networks and prevent unauthorized personnel from accessing your systems.
- ✦ Avoid using employee Social Security numbers for identity numbers and limit access to employees’ private information—including information on medical conditions, claims and disabilities—to a need-to-know basis. Store this information on secure systems, and have those with access to it log off their computers when away from their desks.
- ✦ Dispose of any records containing personal data properly. Shred printed records before discarding. And when disposing of any electronic media (including hard drives), either destroy the media or reformat it—when you simply “erase” data, it just gets overwritten and can be recreated.
- ✦ Develop policies for what kind of information can be worked on at home or on laptops offsite, and take measures to protect data on laptops.
- ✦ Consider buying one of the new identity theft policies for businesses. These policies protect your firm from liability losses when your data is stolen or used by identity thieves. Policies cover direct expenses, such as defense costs, legal damages, fines, regulatory actions and notification costs. Some policies also cover services that protect or help restore your reputation, including public relations counsel and assistance for victims. Group policies that protect your employees from the costs of identity theft are available as well. For more information, contact your account manager at The Addis Group. ■



Evaluating Your Employee Screening Process

by Kevin Conrad

When it comes to finding a company to pre-screen your employees, you have several factors to consider. You have to find a company you feel comfortable with and that you can trust. After all, you will be sending them very sensitive information, with identities of individuals at stake. You also want to ask that company to send you either a sample report or to run a couple of free searches for you so that you can familiarize yourself with their process and get a first-hand look at how thorough their searches are.

If you decide to ask them to run a few free searches for you, make sure that you send them information on someone that you already have results on so that you can check their report against what you already know. Ask them if they are a member of the NAPBS, the National Association of Professional Background Screeners. Most reputable companies are members, and they are proud of it, so they will usually have the NAPBS logo on their site. The easiest way to find a member of NAPBS is to go to their website at www.NAPBS.com, which has a link to help you find a background screening company in your area.

Make sure you ask a lot of questions. Ask them about their online security measures, how you submit your requests, how they return your results, and the process that they

use for ensuring accuracy. Let them know how important this is to you. Have them walk you through the ordering process online for the first couple of searches to make sure that you understand how it all works. They should have no problem giving you a demonstration even before you sign up. Ask if they have a contract, because some companies do and some don't. If they don't have a contract, they should at least have a service agreement that basically says that they are going to abide by the FCRA, and they assume that you are going to do the same.

Find out what other resources they offer. Do they have a glossary of terms? How about downloadable release forms? Check to see if they have downloadable pre-adverse action letters, and adverse action letters. In order to be compliant, you'll need all of these. What are their identifiers to make sure that they have the right person? Are all of their searches done in "real time" or do they rely on databases? If you decide to run a database search, ask them to send you a search description that details everything covered and where the data comes from.

All of these things will help to make sure that you are keeping your employees and clients safe. These days, the only thing you can be sure of is that when it comes to people, you just never know. ■

Kevin Conrad is the president and owner of Complete Security Investigations in Dallas, Texas. He is a licensed private investigator. His contact information is available at www.csidf.com.

Seminar Discusses Employee Theft

Did you know that more than 1 in 3 private companies surveyed reported experiencing employee theft such as stolen funds, equipment, inventory or merchandise within the last three years? Did you know that nearly 25 percent of the cases caused losses of at least \$1 million?

On November 9, 2006 Bradley Baturka of AON Consulting gave an eye-opening presentation on the growing problem of corporate fraud as part of the Risk Management Leadership Series sponsored by The Addis Group. Mr. Baturka warned that in order to avoid being burned by billing schemes, falsification of financial reports, check tampering, illicit wire transfers and other types of fraud, companies need to implement good internal controls. In addition to internal controls, a tip line is critical. When corporate fraud is detected, it is because of a tip in 34 percent of cases. Tips usually come from another employee. Other common anti-fraud measures include fraud awareness or ethics training, internal audits, external audits and surprise audits.

The Addis Group Academy of Risk Management will be releasing its 2007 schedule of events shortly. ■



A Susquehanna Company

THE ADDIS GROUP
2500 RENAISSANCE BOULEVARD
KING OF PRUSSIA, PA 19406-2772

MANAGING RISK Newsletter