Your Monthly Newsletter from Strategic Business Services

Monthly Newsletter

by Strategic Business Services

August 2017

USCIS Releases New Form I-9

U.S. Citizenship and Immigration Services (USCIS) has released a new version of Form I-9, *Employment Eligibility Verification*. **By September 18, 2017, employers must use only the new version**.

Compliance Dates for New Form I-9

The new Form I-9 features a revision date of July 17, 2017. **While employers may continue using a Form I-9 with a revision date of November 14, 2016 through September 17, 2017, as of September 18, 2017, employers must use only the new version.**

Changes to Form I-9

The following revisions have been made to the List of Acceptable Documents section of the new Form I-9:

- The Consular Report of Birth Abroad (Form FS-240) has been added to List C. Employers completing Form I-9 on a computer are now able to select Form FS-240 from the drop-down menus available in List C of Section 2 and Section 3.
- All the certifications of report of birth issued by the U.S. Department of State (Form FS-545, Form DS-1350, and Form FS-240) are now combined into selection C#2 in List C.
- All List C documents have been renumbered except the Social Security card. For example, the employment authorization document issued by the U.S. Department of Homeland Security on List C has changed from List C #8 to List C #7.

For more information on complying with the employment eligibility verification requirements, please visit our Form I-9 section.

Summer's Here and So is Spear Phishing

Cyber attacks and resulting data breaches often begin with a **spear-phishing email**. Spear phishing differs from regular email phishing in its use of extensive research to target a specific audience, which allows the spear phisher to pose as a familiar and trusted entity in its email to a mark. Spear phishers seek a company's valuable information—such as **credentials providing access to customer lists, trade secrets, and confidential employee information**—and some of their methods include:

- Directing email recipients to fake (but authentic-looking) websites that ask for information like account numbers, passwords, or other credentials; and
- Inducing recipients to click on links or attachments that download malware onto the recipient's computer. The malware often allows the phisher to steal passwords and sensitive data by, for example, tracking keystrokes.

The IRS offers the following tips to protect against spear phishing:

1. Educate **all employees** about phishing in general and spear phishing in particular.
2. Use **strong, unique passwords** with a mix of letters, numbers, and special characters. Also, remember to use different passwords for each account.
3. Never take an email from a familiar source at face value, especially if it asks you to open a link or attachment, or includes a threat about a dire consequence that will result if you fail to take action.
4. If an email contains a link, **hover your cursor over the link** to see the web address (URL) destination. If it's not a URL you recognize, or if it's an abbreviated URL, don't open it.
5. Poor grammar and odd wording are **warning signs** of a spear-phishing email.
6. Consider calling the sender to confirm the authenticity of an email you're unsure of, but don't use the phone number in the email.
7. Use security software that updates automatically to help defend against malware, viruses, and known phishing sites.

Check out our Employee Records and Files section for more on how to protect confidential employee information.

5 Guidelines for Protecting Employees from Heat Stress

With the dog days of summer under way, it is critical that employers recognize the hazards of working in hot environments and take steps to reduce the risk to workers. Consider taking the following actions that can help protect employees:

1. **Provide heat stress training.** Topics you may wish to address include worker risk, prevention, symptoms, treatment, and personal protective equipment.
2. **Schedule hot jobs for the cooler part of the day.** The best way to prevent heat illness is to make the work environment cooler. Monitor weather reports daily and reschedule jobs with high heat exposure to cooler times of the day. When possible, routine maintenance and repair projects should be scheduled for the cooler seasons of the year.
3. **Provide rest periods with water breaks.** Provide workers with plenty of cool water in convenient, visible locations in shade or air conditioning that are close to the work area. Avoid alcohol and drinks with large amounts of caffeine or sugar.
4. **Monitor workers who are at risk of heat stress.** Workers are at an increased risk of heat stress when wearing personal protective equipment, when the outside temperature exceeds 70°F, or while working at high energy levels. Establish a routine to periodically check workers for signs and symptoms of overexposure.
5. **Acclimatize workers by exposing them for progressively longer periods to hot work environments.** Allow workers to get used to hot environments by gradually increasing exposure over at least a 5-day work period. The U.S. Occupational Safety and Health Administration (OSHA) suggests beginning with 50% of the normal workload and time spent in the hot environment, and then gradually building up to 100% by the fifth day.

Our section on Safety & Wellness includes additional tips for maintaining a safe and healthy workplace.

MLR Rebates Due to Plan Sponsors by September 30

The Medical Loss Ratio (MLR) rules under Health Care Reform require an issuer to provide rebates if its medical loss ratio (the amount of health insurance premiums spent on health care and activities to improve health care quality) falls short of the applicable standard during a reporting year. **Each year's rebates must be provided by issuers to policyholders (typically the employer that sponsors the plan) by September 30 of the following year.**

Employer Distribution
The MLR rules provide that issuers must pay any rebates owed to persons covered under a group health plan to the policyholder, **who is then responsible for distributing the rebate to eligible plan enrollees**.

In general, there are several ways rebates may be distributed to plan enrollees, including:

- A rebate check in the mail;
- A lump-sum reimbursement to the same account that was used to pay the premium if it was paid by credit card or debit card; or
- A direct reduction in future premiums.

In addition to the above methods, employers may also apply the rebate in a way that benefits employees.

Check out our section on Medical Loss Ratio (MLR) Rebates & Employer Responsibilities to learn more.