Your Monthly Newsletter from Benefit Partners Group, LLC.

Benefit Partners Group

Monthly Newsletter

July 2018

Form 5500 Filing Deadline for Many Health Plans is July 31

Group health plan administrators are reminded that Form 5500 must be filed with the U.S. Department of Labor (DOL) by the last day of the seventh month after the plan year ends. **For calendar-year plans, that due date falls on July 31**.

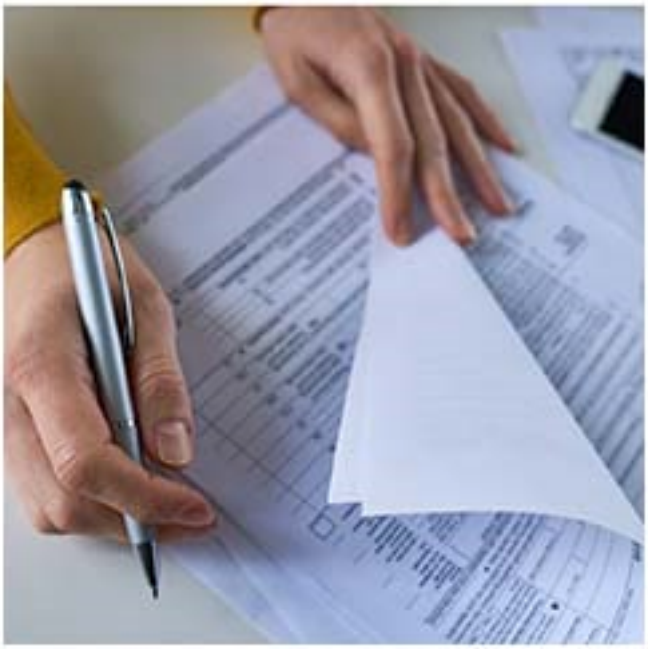
Who Must File Form 5500?
In general, all group health plans covered by the Employee Retirement Income Security Act (ERISA) are required to file Form 5500. However, group health plans (whether fully insured, unfunded [meaning its benefits are paid as needed directly from the general assets of the plan sponsor], or a combination of the two) that covered **fewer than 100 participants** as of the **beginning** of the plan year **are exempt from the Form 5500 filing requirement**. For more on this requirement, click here.

How to File Form 5500

Forms 5500 must be filed electronically with the DOL using either the IFILE web-based filing system or an approved vendor's software.

Visit our ERISA section for more ERISA compliance information.

Form I-9 Audits Up Dramatically Since October



From October 1, 2017-May 4, 2018, U.S. Immigration and Customs Enforcement (ICE) conducted 2,282 Form I-9 audits, up from 1,360 audits from October 1, 2016-September 30, 2017. Given this dramatic increase, employers should take a moment to ensure that their Form I-9 compliance practices meet federal requirements. Businesses that fail to comply with these requirements are subject to penalties of **up to $2,236 per violation**.

4 Quick Form I-9 Compliance Tips

1. All U.S. employers generally must fill out and keep a Form I-9 for every person they hire for employment in the United States, as long as the person works for pay or other benefits.
2. Newly hired employees must complete and sign Section 1 of Form I-9 **no later than the first day of employment**.

3. An employee must present to the employer an original document or documents that show his or her identity and employment authorization **within 3 business days of the date employment begins**.
4. Employers must retain an employee's completed Form I-9 for as long as the individual works for the employer. **However, Form I-9 does not need to be filed with any federal agency**.

For additional Form I-9 compliance information, check out our Form I-9 section.

Don't Forget to Pay PCORI Fees

Employers that sponsor certain self-insured health plans--including some health reimbursement arrangements (HRAs) and health flexible spending arrangements (health FSAs)--are reminded that they are responsible for Patient-Centered Outcomes Research Institute (PCORI) fees. Fees for self-insured plans with plan years that ended in 2017 are due **July 31**, and are required to be paid via IRS Form 720.

Employer-sponsored self-insured plans with plan years that ended **between January 1, 2017 and September 30, 2017** must pay a fee of $2.26 multiplied by the average number of lives covered under the plan. Employer-sponsored self-insured plans with plan years that ended **between October 1, 2017 and**

December 31, 2017 must pay a fee of $2.39 multiplied by the average number of lives covered under the plan. Details on how to determine the average number of lives covered under a plan are included in these regulations.

For additional information, visit our section on PCORI Fees for Self-Insured Plans.

Summer's Here and So is Spear Phishing

Cyberattacks 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.
- 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.

Click here for additional information about protecting yourself from spear-phishing attacks.

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

HR Action Steps for Employee Name Changes