



MINDING YOUR Ps AND Qs WHEN DEALING WITH PEOs—Insurance Implications for Clients of Professional Employer Organizations

With all the headaches associated with staying on top of changing labor and employment laws, it is no surprise that employers of all sizes are outsourcing their Human Resources functions to Professional Employer Organizations or “PEOs.” A PEO is a third-party company that enters into a co-employer relationship with a client-employer. In creating a co-employer relationship, both the PEO and the client-employer share and manage many employer-related liabilities and responsibilities. Typically, the co-employment relationship is based on a contract between the PEO and the company outlining the PEO’s responsibilities (e.g., payroll, benefits administration, leave administration and other HR functions) and the company’s responsibilities (e.g., day-to-day supervision of workers, control over hiring, firing, and terms and conditions of employment).

PEOs come in all sizes and shapes, from payroll-only services to an off-site, full service Human Resources department. PEOs often market their services to client-employers as means to cut costs, improve efficiency, and ensure compliance with state and federal workplace legislation. Client-employers also benefit from entering into a PEO relationship because PEOs have the ability to spread costs of employee benefits among all of its clients and offer a wider selection of benefits.

In contrast to temporary staffing firms which place their own employees at a customer’s place of business to perform services for the client-employer’s place of business, PEOs do not have their own workforce and ostensibly assume only administrative functions for its client-employers such as payroll and benefits coverage and administration, e.g., workers’ compensation and health insurance. PEOs typically have no direct responsibility over the employees of its clients, including hiring, training, supervision, evaluation, discipline or discharge, among other critical employer functions.

This distinction became significant on January 16, 2009, when the United States Department of Labor implemented specific changes to the Family and Medical Leave Act (“FMLA”) affecting employers in a PEO relationship. Employers with 50 or more employees are covered by the FMLA. If two entities are considered “joint

employers,” each employer must include the employees of both entities in determining whether the 50-employee threshold has been met.

Previously, PEOs were considered “joint employers” of the client’s workers and were counted towards the 50-employee minimum for the FMLA. As the primary employer, the PEO was required to provide required FMLA notices to its employees, providing FMLA leave, maintaining group health insurance benefits during the leave, and restoring the employee to the same or equivalent job upon return from leave. As the secondary employer, the client-employer would be responsible for accepting the employee returning from FMLA leave if the PEO chose to place the employee with the client-employer. See Wage and Hour Opinion Letter FMLA-111 (September 11, 2000).

The new DOL regulation now provides that employees of a PEO are not considered in the 50-employee count if the PEO merely performs administrative functions such as payroll, benefits administration, and the like. 29 CFR § 825.106(b)(2). The determination of whether the PEO is a “joint employer” is based on the economic realities and specific facts and circumstances of the relationship. If the PEO has the right to hire, fire, assign or direct and control the client employer’s employees, it would be considered a “joint employer” with the client-employer. In circumstances where there is “joint employer” status, the client-employer will generally be regarded as the primary employer. This change is significant as the primary employer is responsible for giving employees the required FMLA notices providing FMLA leave and maintaining any health benefits. Until this change, the primary employer was considered to be the PEO.

Notwithstanding this newly forged distinction, employees will sue both the PEO and the client-employer as “joint employers” for, e.g., wrongful termination, violation of anti-discrimination laws, breach of fiduciary duty owed in implementing 401(k)s or health benefit programs, and so on. In such circumstances, the PEO will contend it was not the plaintiff’s “employer” because it did not exercise

(continued, next page)



Breach Notification Requirements under HIPAA Page 3

MINDING YOUR Ps AND Qs (cont.)

sufficient right of control over the worksite employees to be deemed an employer. *Nationwide Mutual Ins. Co. v. Darden*, 531 U.S. 318 (1992). Indeed, courts in various situations have found that PEOs and staffing agencies are not common-law employers of their client's employees. *Takacs v. Fiore*, 473 F.Supp.2d 647 (D.Md.2007) (sexual harassment); *Salley v. PBS of Central Florida, Inc.*, 2007 U.S. Dist. LEXIS 91212 (M.D. Fla. 2007) (FLSA); *Boston Old Colony Ins. Co. v. Tiner Assoc., Inc.*, 288 F.3d 222 (5th Cir. 2002) (negligence). Thus, in line with the new FMLA regulations, PEOs will not be considered "joint employers" if they did not supervise client's employees or control their day-to-day activities.

In defending against employee-lawsuits, PEOs will also rely upon the indemnification provision contained in the PEO/client services contract to shift responsibility to the client-employer. In this fashion, it is important for the client-employer to understand the rights and duties contained in the PEO/client services agreement, the scope of services to be offered by the PEO, and importantly, the insurance implications when contracting with a PEO.

Some PEOs will purchase Employment Practices Liability Insurance ("EPL") protecting themselves and the client-employer as insureds under the policy. This insurance provides defense and indemnity for employment-related lawsuits alleging wrongful termination, sexual harassment, discrimination and other such actions. While a desirable feature, there are potential pitfalls to relying solely upon the PEO-provided Employment Practices Liability Insurance including the following:

- ◆ **Inadequate Limits.** With the average defense costs of employment-related claims in the tens of thousands of dollars and the average EEOC settlement exceeding \$200,000, the typical limits of the PEO-provided EPL insurance may prove insufficient to deal with larger claims or multiple claims during the course of the year.
- ◆ **Lack of Control of the Policy.** Unlike an employer's Property, General Liability and related insurance over which they have control of the placement and claims process, in the case of PEO-provided EPL coverage, companies have no control over the policy. This can create significant issues including:

- ~ **Policy Definitions and Exclusions.** The inability of the PEO to negotiate terms specific to the client-employer may result in some entities or persons without coverage. For example, some EPL forms may not include non-compensated officers as

insured persons or natural persons who are working for the employer but not paid through the PEO's payroll system. Lacking such coverage, these persons and the employer itself could find themselves without coverage. And many PEO-provided EPL forms do not include subsidiaries in the definition of entities insured under the policy which likewise may create a coverage gap for subsidiary operations of PEO Clients.

- ~ **The Claims Process.** Claims generally must be submitted to the PEO who will in turn submit these claims to the insurer. The client-employer generally would not have the right to consent to the law firm representing the claim but would use the firm selected by the PEO and the insurer. And some PEO-employer EPL forms have included exclusions related to failure to comply with policies and procedures in the employee manual which could eliminate coverage for allegations of intentional acts (e.g., allegations of sexual harassment would be considered intentional acts; were an EPL policy to preclude coverage for failure to comply with promulgated policies and procedures, including policies related to harassment and discrimination, coverage could be denied for such claims).

- ~ **Policy Termination.** As the EPL coverage is placed through the PEO as part of their service contract, termination of the PEO/client service agreement with the PEO will likely result in loss of EPL coverage thereby leaving the client-employer uninsured unless other EPL insurance has been secured prior to the termination of the PEO contract. Similarly the PEO or the insurer may elect to terminate or restrict coverage and, further, under the terms of the policy may not be required to advise the client of the changes in terms or cancellation of coverage.

- ◆ **Emerging Exposures.** Defense coverage for wage and hour related action and immigration has been difficult to obtain in recent years but such is becoming much more readily available in the insurance market. However, underwriters are generally not providing these extensions on a blanket basis but subject to individual account underwriting. PEO-provided EPL insurance may lack this important coverage.
- ◆ **Lack of Third-Party EPL Coverage.** Coverage for non-employee third parties for claims alleging discrimination or harassment has become fairly common in the broader EPL Insurance market but such coverage may not be included via the PEO-provided EPL coverage.

In addition to presenting challenges in insurance policy administration as respects EPL insurance coverage, the PEO relationship may arguably create additional duties related to compliance with laws and regulations for the client-employers. For example, under California Government Code section 12950.1, an employer with fewer than 50 employees in California would not be required to provide sexual-harassment prevention training to its staff as required by statute. But as a member of a PEO who employs hundreds if not thousands of individuals, such training may be necessary to comply with the law given the ambiguity of the “joint employer”—unlike the recent “carve out” described above under the FMLA. Therefore, the “joint employer” relationship between PEOs and their client-employers may be obligating employers to comply with regulations principally intended for larger companies.

In order to best manage these exposures, clients of PEOs should carefully review the scope of services to be provided by the PEO and indemnification provisions in their PEO contract and may wish to engage outside counsel to ensure that any such indemnification is appropriate to the needs of the client-employer. Additionally, client-employers should review and understand their duties and obligations related to any EPL coverage in place through the PEO to ensure that they protect coverage by complying with any claims notice and related provisions of the policy. And rather than solely relying upon Employment Practices Liability Insurance afforded via the PEO (assuming such is in effect), employers should work with their insurance representative to secure their own EPL coverage, either on a stand-alone basis, or as part of a broader Management Liability program.

-By Katherine S Catlos, Esq., Kaufman Dolowich Voluck & Gonzo LLP and William Dougherty, Hays Companies, Assistant Vice President of Property and Casualty

This article originally appeared in the September 2009 issue of the PLUS Journal. It is reprinted here with permission.

SUMMARY OF BREACH NOTIFICATION REQUIREMENTS UNDER HIPAA

The Health Information Technology for Economic and Clinical Health (HITECH) Act, part of the American Reinvestment and Recovery Act (ARRA) of 2009, made changes to HIPAA Privacy and Security requirements. It expands notification requirements in the event of a security breach, **effective September 23, 2009**.

BREACH AND UNSECURED HEALTH INFORMATION DEFINITIONS

Breach—an unauthorized acquisition, access, use or disclosure of Protected Health Information (PHI) that

compromises the information’s security or privacy.

Unsecured PHI—PHI that is not secured by using a technology or methodology specified by Health and Human Services (HHS). HHS released guidance on April 27, 2009 specifying technologies and methodologies for rendering PHI unreadable and unusable. A copy of the guidance is available at: <http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/federalregisterbreachrfi.pdf>

The following events are excluded from the definition of a breach:

- ◆ When the unauthorized person to whom the information is disclosed would not reasonably be able to retain it.
- ◆ When the breach results from an unintentional action by an employee or other person acting under authority of a covered entity (or business associate) and the action was taken in good faith and within the scope of employment or other professional relationship; and the information is not further acquired, accessed, used or disclosed by any person.
- ◆ The disclosure was inadvertent and from an individual otherwise authorized to access PHI at a facility operated by a covered entity (or business associate) to a similarly situated person at the same facility, and the information is not further acquired, accessed, used or disclosed without authorization by any person.

RISK ASSESSMENT

To determine if an impermissible use or disclosure of protected health information constitutes a breach, covered entities and business associates will need to perform a risk assessment to determine if there is a significant risk of harm to the individual as a result of the impermissible use or disclosure. Did the breach compromise the security or privacy of PHI? Does the breach pose a significant risk of financial, reputational, or other harm to the individual? Who impermissibly used or to whom the information was impermissibly disclosed?

If PHI is impermissibly disclosed to another entity subject to the HIPAA Privacy and Security Rules there may be less risk of harm to the individual because the recipient entity is obligated to protect the privacy and security of the information it received. But if PHI is impermissibly disclosed to any entity or person that does not have similar obligations to maintain the privacy and security of the information, the risk of harm to the individual is much greater and a breach has occurred.

For example, there may be circumstances where a covered entity takes immediate steps to mitigate an

BREACH NOTIFICATION, (cont.)

impermissible use or disclosure, such as by obtaining the recipient's satisfactory assurances that the information will not be further used or disclosed or will be destroyed. This may be addressed through the use of a confidentiality agreement or similar means. If such steps eliminate or reduce the risk of harm to the individual to a less than "significant risk," then HHS interprets that the security and privacy of the information has not been compromised and, therefore, no breach has occurred.

Another example where a breach has not occurred may be when a laptop is lost or stolen and then recovered. If a forensic analysis of the computer shows that its information was not opened, altered, transferred, or otherwise compromised, such a breach may not pose a significant risk of harm to the individuals whose information was on the laptop. However, if a computer is lost or stolen, it is not considered reasonable to delay breach notification based on the hope that the computer will be recovered.

If the risk assessment indicates that a breach has occurred, the breach notification requirements will apply.

BREACH NOTIFICATION REQUIREMENTS

Group health plans and other covered entities must notify each individual whose *unsecured* PHI has been, or is reasonably believed by the covered entity to have been, accessed, acquired or disclosed as a result of a breach. Notice of a breach must be provided to each affected individual via first-class mail at the individual's last known address, or by e-mail if the individual specifically indicated a preference for e-mail notices. A copy of the interim final rules is available at <http://edocket.access.gpo.gov/2009/pdf/E9-20169.pdf>.

Notice must be provided without unreasonable delay, and in no case later than 60 calendar days after the breach is discovered. The time for reporting the breach begins when a breach is discovered. A breach is treated as discovered by the covered entity (or business associate) as of the first day on which the entity (or business associate) finds out the breach has occurred, or

reasonably should have known that it occurred.

If the breach involves more than 500 residents of a specific state or jurisdiction, notice must be provided to prominent media outlets in the state or other jurisdiction. The covered entity must also notify the Department of Health and Human Services (HHS) immediately if the breach affected 500 or more individuals — which in turn must post information about the breach on the agency's web site. If a business associate (as defined by HIPAA) is responsible for a breach, the business associate must notify the covered entity of the breach, listing each individual whose PHI was, or is reasonably believed to have been, accessed, acquired or disclosed.

HHS released interim final rules August 24, 2009, effective September 23, 2009. The notification must include, to the extent possible:

- ◆ A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;
- ◆ A description of the types of unsecured protected health information that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);
- ◆ Any steps individuals should take to protect themselves from potential harm resulting from the breach;
- ◆ A brief description of what the covered entity involved is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and
- ◆ Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Web site, or postal address.

-Ben Graves, Associate Director of Compliance & Research, Hays Companies' Benefits



HAYS COMPANIES
IDS Center, Suite 700
80 S 8th Street
Minneapolis, MN 55402

Locally Owned, Globally Connected, Serving the needs of our customers: Risk Management, Insurance, Employee Benefits and Retirement Planning.

With Offices in 19 U.S. cities—For a complete listing, please consult our website at www.hayscompanies.com.

THIS NEWSLETTER IS A PERIODIC PUBLICATION OF HAYS COMPANIES. THE CONTENTS ARE INTENDED FOR GENERAL INFORMATION PURPOSES ONLY AND SHOULD NOT BE CONSIDERED LEGAL ADVICE OR LEGAL OPINION ON ANY SPECIFIC FACTS OR CIRCUMSTANCES. YOU ARE URGED TO CONSULT YOUR CORPORATE COUNSEL OR BENEFITS ATTORNEY CONCERNING ANY LEGAL QUESTIONS YOU MAY HAVE.