



## RULINGS, OPINIONS, ETC.

### **HHS Issues Interim Final Rules on HIPAA Breach Notification.**

The Department of Health and Human Services (HHS) issued interim final rules regarding the Health Insurance Portability and Accountability Act's (HIPAA's) breach notification requirement. The breach notification mandate, included in HIPAA as part of the American Recovery and Reinvestment Act, requires covered entities (health plans, health care providers, and health care clearing houses) to notify individuals affected by breaches of their unsecured protected health information (PHI).

The interim final rules define a "breach" as "the acquisition, access, use, or disclosure of PHI in a manner not permitted [by the privacy regulations] which compromises the security or privacy of the PHI." Not every impermissible use or disclosure of PHI will be considered a breach subject to the notification requirements. The interim final rules provide that a breach will compromise security only if it poses a "significant risk" of financial, reputational, or other harm to the individual. When determining whether a disclosure poses a significant risk of harm, covered entities should consider the type and amount of PHI disclosed, the identity of the unauthorized person who disclosed the PHI, and whether steps have been taken to mitigate harm.

In addition to adding the "significant risk" threshold, the interim final rules also provide three exceptions to the duty to notify individuals when there has been a breach of their PHI. These exceptions are:

- Any unintentional acquisition, access, or use of PHI by an employee of a covered entity or business associate. This exception applies to acquisition, access, or use that occurs within the normal scope of employment, is done in good faith, and does not lead to further use or disclosure.
- Any inadvertent disclosure from a person authorized to access PHI at a covered entity or business associate to another similarly authorized person. For this exception to apply, the PHI must not be further used or disclosed in a manner not permitted by the privacy rules.
- A disclosure to an unauthorized person who could not reasonably have retained the disclosed PHI. For example, if a plan participant's explanation of benefits is accidentally mailed to the wrong individual, but the envelope is returned to the covered entity unopened.

To comply with the breach notification rules, whenever there is a potential breach, covered entities should perform and document a risk assessment of each event to determine:

- If the use or disclosure of PHI violated the HIPAA privacy rules;
- If the impermissible use or disclosure involved unsecured PHI;
- If the impermissible use or disclosure of unsecured PHI met the significant risk standard and therefore qualifies as a breach; and
- If the breach meets any of the regulatory exceptions to notification.

In the event there is a breach and it does not qualify as an exception, covered entities must notify individuals affected by the breach without unreasonable delay and in no event later than 60 days from the date the breach is discovered.

In addition to the affected individuals, HHS (and in some cases prominent media outlets) must also be notified. The timing of the notification depends on the number of individuals affected by the breach. If the breach involved 500 or more individuals, HHS must be notified at the same time as the individuals affected by the breach (i.e., without unreasonable delay and in no event later than 60 days from the date the breach is discovered). If the breach involved 500 or more individuals from the same state or jurisdiction, prominent media outlets serving that area must also be notified within this timeframe. If the breach involved fewer than 500 individuals, the breach must be recorded and a log documenting the breach must be provided to HHS within 60 days following the end of the calendar year.

Also, if the covered entity cannot notify 10 or more individuals affected by the breach because they cannot be located, the covered entity must provide substitute notice by conspicuously publishing the notice on the covered entity's Web site or in a prominent media source that serves the affected geographic area. In addition, the covered entity must establish a toll-free number and make it available for 90 days for the affected individuals to obtain information about the breach.

Business associates must notify the covered entity within 60 days of discovering a breach of unsecured PHI. Although business associates are not required by the regulation to notify the affected individuals directly, a covered entity could

---

impose such a requirement under the terms of a business associate agreement.

Although the breach notification rules became effective on September 23, 2009, HHS stated that it will not impose sanctions under the new rules until February 22, 2010. This delay is intended to give covered entities and business associates time to comply with the new rules by formulating risk assessment procedures, amending their privacy and security policies, training employees, and reviewing business associate agreements for breach notification provisions. (74 Fed. Reg. 42740)

### **Is Your Health Risk Assessment Compliant With GINA?**

The Genetic Information Nondiscrimination Act of 2008 (GINA) prohibits group health plans from discriminating based on genetic information. Final regulations implementing GINA were issued by the Departments of Labor, Health and Human Services, and Treasury in October of this year, effective for plan years beginning on or after December 7, 2009 (January 1, 2009 for calendar year plans). The new regulations amend HIPAA, ERISA's nondiscrimination rules, and the Internal Revenue Code.

Under GINA, group health plans and health insurance issuers may not (among other prohibitions) collect "genetic information" either before or in connection with enrollment, or for underwriting purposes. "Genetic information" is defined to include an individual's own genetic tests, genetic tests relating to family members, and the manifestation of a disease or disorder in the individual's family members (i.e., family medical history).

Most wellness and disease management programs that utilize health risk assessments are likely to be directly impacted. A health risk assessment that does not directly request genetic information, and is not designed to solicit such information, will not violate GINA even if completion of the assessment is connected to a reward or other benefit. However, most health risk assessments currently in use directly request (or are designed to solicit) information regarding an employee's family medical history. As such, all such questionnaires will need to be carefully reviewed for compliance with GINA.

Not all health risk assessments that request genetic information are problematic. Under GINA, genetic information may be collected as part of a health risk assessment as long as no rewards are provided, the health risk assessment does not prompt individuals to provide genetic information, and the request is not made prior to or in connection with enrollment.

What should employers do?

- Review health risk assessment questionnaires and other plan enrollment materials to determine if they directly solicit genetic information or are worded in

such a way as to prompt a participant to provide such information. Any questions that could reasonably prompt an employee to provide genetic information should specifically (and prominently) direct the employee to refrain from including information related to genetic testing, genetic services, genetic counseling, or genetic diseases for which they believe they may be at risk.

- Confirm that your third-party administrators, wellness program vendors, and insurance carriers are aware of GINA's prohibitions and are prepared to represent that they are in full compliance with them. Seek or expand hold harmless provisions from vendors and insurance carriers to address the compliance risks associated with GINA violations.

### **Transfer Unused Leave Time to 401(k).**

The IRS has issued two revenue rulings that will facilitate the use of deferrals in 401(k) plans as an alternative to paying out unused vacation or sick leave to employees. It is not unusual for an employer to cash out unused leave time either on an annual basis for current employees or at separation from service for a terminating employee. While the rulings do not change the rules for 401(k) deferrals that are either nonelective employer contributions or participant-elected deferrals, the rulings are designed to clarify and facilitate increased retirement savings by describing how unused leave time can be transferred into a 401(k) account. One ruling deals with ongoing plan participants and provides guidance on how a 401(k) plan may be amended to permit or require that the dollar value of unused leave time or paid time off be contributed to a participant's 401(k) account. Some employers may cash out this unused leave time and others may forfeit it. If the participant would otherwise receive a cash-out, the amount available could be deferred in a 401(k) plan. The amount counts as "compensation" for purposes of the limits on 401(k) contributions and deferrals. An employer could require that the value of the unused leave be contributed to the plan as a nonelective employer contribution. These amounts would be subject to nondiscrimination testing applicable to either elective deferrals or employer contributions. The second ruling deals with the same issues in the context of a terminating employee. So long as the unused leave time is paid out or deferred in a plan by the later of two and a half months after severance from employment or by the end of the year in which severance occurred, the value of the unused leave may be deferred in a 401(k) account. (Rev. Ruls. 2009-31, 2009-2.)

### **IRS Publishes Safe Harbor Eligible Rollover Distribution**

**Notices.** A plan administrator of a qualified retirement plan is required to provide a written explanation to any recipient of an eligible rollover distribution. The written explanation generally must describe the direct rollover rules, the mandatory income

tax withholding rules for distributions not directly rolled over, the tax treatment of distributions not rolled over, and when distributions may be subject to different restrictions and tax consequences after being rolled over. The Internal Revenue Service (IRS) previously published a safe harbor notice plan administrators could use to satisfy this notice requirement, but the safe harbor notice was last published in 2002 and had become outdated.

On September 5, 2009, the IRS published IRS Notice 2009-68, which contains two safe harbor explanations that may be provided to recipients of eligible rollover distributions. A principal purpose of the changes in the new safe harbor explanations is to simplify the presentation and description of the participant's options upon receiving an eligible rollover distribution. The new safe harbor explanations also broaden the information to reflect changes in law, such as information on a distribution from a designated Roth account under an employer plan.

There are two safe harbor explanations in the notice. One safe harbor explanation does not include information relevant to distributions from a designated Roth account. That safe harbor explanation should be used only for a distribution that is not from a designated Roth account. The other safe harbor explanation reflects the rules relating to distributions from a designated Roth account and should be used only for a distribution from a designated Roth account. Both explanations should be provided to a participant if the participant is eligible to receive eligible rollover distributions both from a designated Roth account and from an account other than a designated Roth account. A plan may customize the safe harbor explanation by omitting any information that does not apply to the plan.

The new safe harbor explanations may be used immediately. However, the 2002 safe harbor explanations published in IRS Notice 2002-3, appropriately modified to reflect subsequent statutory changes, will continue to be safe harbor explanations with respect to explanations provided through December 31, 2009.

#### **Guidance on "Escalator" Features in 401(k) Plans.**

The IRS recently published guidance concerning "escalator" features under automatic contribution arrangements in a 401(k) plan. Revenue Ruling 2009-30 addresses two issues:

*1. Will default contributions to a profit-sharing plan fail to be considered elective contributions merely because they are made pursuant to an automatic contribution arrangement under which an eligible employee's default contribution percentage automatically increases or escalates after the first plan year of the eligible employee's participation based in part on increases in the eligible employee's plan compensation?*

Ruling: The contributions in this situation are elective contributions even though the contributions are made pursuant to a default election in the absence of an affirmative election. Because a default contribution percentage can be increased or otherwise changed over time pursuant to a plan-specified schedule, the default contributions in this situation do not cease to be elective contributions merely because default contribution percentages increase over time and such increases are, in part, determined by reference to the amount of, and are scheduled to take effect at or by reference to the time of, future increases in base pay. The IRS also noted that because the automatic contribution arrangement in this situation is not intended to be an eligible automatic contribution arrangement or a qualified automatic contribution arrangement, nonuniformity with respect to increases in the default contribution percentage is permissible.

*2. Will default contributions under an automatic contribution arrangement fail to satisfy the qualified percentage requirement (including uniformity and minimum percentage requirements) relating to a "qualified automatic contribution arrangement" under section 401(k)(13) of the Internal Revenue Code (providing an automatic enrollment nondiscrimination safe harbor) or the uniformity requirement relating to an "eligible automatic contribution arrangement" under section 414(w) of the Internal Revenue Code (permitting 90-day withdrawals) merely because default contributions are made pursuant to an arrangement under which the default contribution percentage for all eligible employees increases on a date other than the first day of a plan year?*

Ruling: Default contributions under an automatic contribution arrangement will not fail to satisfy the qualified percentage requirement (including uniformity and minimum percentage requirements) relating to a qualified automatic contribution arrangement or the uniformity requirement relating to an eligible automatic contribution arrangement merely because default contributions are made pursuant to an arrangement under which the default contribution percentage for all eligible employees increases on a date other than the first day of a plan year.

#### **Employee benefits practice group**

Peter K. Bradley pbradley@hodgsonruss.com

Anita Costello Greer anita\_greer@hodgsonruss.com

Michael J. Flanagan mflanagan@hodgsonruss.com

Richard W. Kaiser rkaiser@hodgsonruss.com

Arthur A. Marrapese, III Art\_Marrapese@hodgsonruss.com

Daniel R. Sharpe dsharpe@hodgsonruss.com

The Guaranty Building, 140 Pearl Street, Suite 100 Buffalo, NY 14202  
Tel: 716.856.4000 Fax: 716.849.0349