

# Benefits Alert

October 2009

## Final Regs Implement HIPAA's Security Breach Rules

Interim final regulations establish the rules with which covered entities (e.g., group health plans and health care providers) and business associates (e.g., third-party administrators of health flexible spending accounts) must comply if there is a breach of the privacy rules under the Health Insurance Portability and Accountability Act (HIPAA). The regs, which became effective September 23, 2009, also provide a 180-day grace period, so only violations that occur on or after February 23, 2010, may result in enforcement action.

### SECURITY BREACHES COVERED

The security breach rules apply when the security or privacy of individuals' protected health

information (PHI) is breached due to an impermissible acquisition, use, or disclosure. PHI is individually identifiable health information that's transmitted or maintained in any form or medium (i.e., paper or electronic records). PHI includes employees' Social Security numbers, dates of birth, and e-mail addresses. However, not every instance of impermissible use or disclosure is a breach of HIPAA's privacy rules that would trigger the security breach rules.

- Impermissible use or disclosure of information that's not PHI isn't a breach of HIPAA's privacy rules.

- There's no breach if PHI is de-identified according to existing HIPAA guidelines — that is, it's encrypted or properly

### In This Issue

- Final Regs Implement HIPAA's Security Breach Rules
- IRS Outlines 401(k) Audit Strategies
- Open Enrollment Is Coming (Gulp!)
- Employers Can Lower Health Plan Costs With Goal-Oriented Wellness Programs

destroyed.

- Breaches that are unintentional, inadvertent, or made in good faith aren't privacy breaches.

Privacy breaches that don't fall into the three bulleted categories still don't trigger the security breach rules if they don't compromise the PHI's security or privacy. A breach compromises security or privacy if it poses a significant risk of financial, reputational, or other harm to the individual. To make this determination, covered entities



Robert S. Golden  
M. Dennis Guappone  
Stephen H. Peck

*Expertise*  
*Innovation*  
*Excellence*

181 Wells Avenue  
Newton, MA 02459  
Phone: (617) 969-0100  
[www.ubserv.com](http://www.ubserv.com)

# Benefits Alert

## Final Regs Implement HIPAA's Security Breach Rules (cont.)

and business associates must perform a risk analysis. The key to this risk analysis is the type and amount of PHI that's involved in the impermissible use or disclosure. If, at the end of the risk assessment, covered entities or business associates conclude that the breach was insignificant, then no breach would be considered to have occurred, and the privacy rule would not have been violated. Covered entities and business associates should document these efforts.

### NOTIFICATION DUTIES

Once a significant breach occurs, covered entities must notify the affected individuals without unreasonable delay and, in any case, no later than 60 calendar days after the breach. Business associates who experience breaches must notify covered entities, so the covered entities can notify the individuals. Covered entities and business associates are treated as having discovered the breach as of the first day on which the breach is actually known, or by exercising reasonable diligence, would have been known to any person, other than the person committing the breach, who is an employee, volunteer, trainee, or other person who is under the covered entities' direct control. *Important:* These rules don't override more restrictive state laws.

If a breach involves 500 or more residents of a state, covered entities must also notify prominent media outlets serving the state, and the Department of Health and Human

Services (HHS). If breaches involve fewer than 500 individuals, covered entities must keep a log of the breaches and notify the HHS within 60 days after the end of each calendar year. Law enforcement agencies may make a written request to delay notification indefinitely; oral requests for delays may be honored for up to 30 days.

Individuals' notification must be written in plain language and sent by first-class mail. Alternatively, individuals may choose to receive notification electronically. If notification is returned as undeliverable, covered entities must send substitute notices that are reasonably designed to reach the individuals. If fewer than 10 notices are returned as undeliverable, covered entities must provide an alternative to written notice, such as notification by phone. If 10 or more notices are returned, covered entities must post a conspicuous notice on their home pages for 90 days, or take out conspicuous notices in major newspapers or notify broadcast outlets in the geographic area where the individuals are likely to reside.

Notification must include a brief description of what happened; a description of the types of unsecured PHI that was breached; the steps individuals should take to protect themselves; a brief description of what the covered entity is doing to investigate the breach, to mitigate harm to individuals, and to protect against further breaches; and contact procedures for individuals to ask questions or learn additional information.

### WHAT TO DO NOW

Covered entities and business associates should use the grace period to take the following steps.

- Train employees and others to determine and document whether there has been an impermissible use or disclosure of PHI.
- Establish risk assessment procedures.
- Ensure that individuals' current addresses, phone numbers, and e-mail addresses are current.
- Review and update service contracts, as necessary, to account for the obligations these regs impose. ❖

\* \* \* \* \*

## IRS Outlines 401(k) Audit Strategies

IRS auditors rarely show up at an employer's establishment cold. They've done their homework, and they've checked it twice. However, a knock on your door doesn't have to result in panic.

### INTERNAL CONTROLS

Auditors have been advised to initially inquire about a plan's internal controls. Auditors who find that a plan lacks sufficient internal controls are further advised to conduct a more thorough examination of the plan. Questions are broken into four broad categories.

- HR — these questions allow auditors to obtain an overview of how HR and the plan

## Open Enrollment Is Coming (Gulp!)

**C**ongressional action regarding health care reform will not affect group health premiums and costs for 2010. For 2009, the combined average premium and out-of-pocket costs for health coverage increased about 9%, according to an annual study conducted by Hewitt Associates. Costs will rise again next year, which means that employees may be looking to change their health benefits. In addition, employers will continue to shift even more of the cost of health benefits to employees in 2010, Hewitt says. And to whom will employees be looking for advice as they negotiate next year's benefits offerings? Sixty-three percent of employees surveyed by MetLife said that they turn to HR and Benefits for guidance. It's time to ramp up your communications apparatus.

### KNOWLEDGE IS POWER

Health care options change

\* \* \* \* \*

### IRS Outlines 401(k) Audit Strategies (cont.)

administrator communicate, as well as the records system used to operate the plan.

- Payroll—these questions inform auditors of how payroll is handled and communicated to the plan administrator.

- Plan failures — auditors assess how a plan failure impacts the plan's internal controls. Auditors are advised to ask these questions early in the audit. The IRS is particularly interested to

every year, even though, according to the MetLife survey, only 25% of employees change their benefits. Worse, 25% of employees expressed confusion about their options and another 24% were frustrated while choosing their benefits. Those feelings won't subside anytime soon. *Reasons:* Since employers have gone about as far as they can in increasing everyone's costs, more targeted increases seem to be the trend. For example, plans are instituting co-insurance payments, in addition to co-payments. Plans are changing prescription drug benefits; are lowering the limits on specialty treatments, appliances, and prostheses; and are carving out annual deductibles from the maximum out-of-pocket expense amounts. Finally, what used to be a part of core benefits — disability and dental insurance, for example — are now being offered *à la carte*,

know whether a correction was considered for all plan years, and whether improvements or enhancements to internal controls will avert similar errors in the future.

- Plan administration — auditors want an idea of the internal controls that are related to plan administration, including communication between the sponsor, the third-party administrator, and the record-keeper. ♦

which means that employees will need to make even more choices.

These targeted changes are aimed at making employees who use more health care pay more. But they're often included in the fine print, which can trap employees who don't read materials carefully or who don't know the lingo. This isn't a good development for already confused or frustrated employees. It's crucial, therefore, that you understand all the fine print.

### TALK TO ME, PLEASE

Once you have that fine print under your belt, you must reach out to employees and their spouses. And they'll be waiting — 27% of employees in the MetLife survey said that they planned on acting on HR's advice.

- **FAQs.** Annual changes to current health benefits can be communicated in a frequently-asked-questions sheet that's distributed or e-mailed to employees, and posted on the employer's website. *Tip:* Be sure to include an e-mail address for employees who have follow-up questions.

- **Keep it simple and personal.** New benefits offerings need a more coordinated roll out. The material you give to employees should be written as simply as possible. *Tip:* Since preprinted brochures from health insurers often fall short of the keep-it-simple rule, and contain that dreaded fine print, create supplementary materials that show how a typical employee "like them" would fare among the various options. And don't undersell cost-shifting mechanisms; doing so can lead employees to feel they were

## Employers Can Lower Health Plan Costs With Goal-Oriented Wellness Programs

The rising cost of employer-provided health benefits is driving more employers to embrace high-deductible health plans that are coupled with goal-oriented wellness programs. Under these programs, employees can take a chunk off of their annual premiums and other out-of-pocket costs by meeting reasonable health goals. But these types of wellness programs, unlike participation-only programs, come with some additional strings, thanks to the Health Insurance Portability and Accountability Act (HIPAA).

### WHAT YOU NEED TO KNOW ABOUT GOAL-ORIENTED PROGRAMS

Goal-oriented wellness programs work best when the program's aim is to alter employees' unhealthy lifestyles. For example, wellness programs typically help employees quit smoking. Goal-oriented programs will work, but less effectively, if you're targeting an underlying health condition. High cholesterol, high blood pressure, and obesity, for example, can be the result of an unhealthy lifestyle or genetics, depending on the individual.

\* \* \* \* \*

### Open Enrollment Is Coming (Gulp!) (cont.)

shortchanged.

- **Make communication continuous.** Nearly 66% of employees in the MetLife survey said that meetings were helpful to them. But meetings usually aren't enough. *Tip:* Supplement group meetings with one-on-one chats, periodic e-mails, easy-to-use web-based calculators and tools (no burying information three screens down from the home page), and even a benefits blog that, say, you contribute to on a weekly basis. Also, make materials available to employees throughout the year.

#### NEXT STEPS

Don't provide employees with materials and expect them to

review everything right away. Employees will have questions regarding new plans or new plan options. Alert your staff to expect an increase in phone calls and e-mails, especially on Mondays, after employees and their spouses have a weekend to dig through the material you've provided.

As for the open enrollment process itself, ditch the paper forms and try online or telephone enrollment. Whatever you do, don't pick Friday as your enrollment deadline. Experience shows that Friday deadlines only increase Monday morning phone calls. Monday deadlines are equally undesirable; Wednesday seems to be best. ❖

HIPAA takes the lifestyle choice vs. underlying medical condition into account by imposing five standards that all goal-oriented wellness programs must meet; failure to meet these five standards can result in tax penalties.

- The total reward given to employees under all wellness programs must be limited to 20% of the total cost of coverage (i.e., employer and employee contributions).

- The program must be *reasonably* designed to promote health and prevent disease. The reasonably-designed standard must be flexible. Smokers, for example, don't necessarily have to quit to earn their reward. Similarly, obese employees don't have to lose weight; it's the trying that's important. Also, the program should offer participants a reasonable chance of improving their health, but doesn't need to be overly burdensome.

- Participants must be allowed to qualify for the reward at least once a year.

- Reasonable alternative standards for obtaining the reward must be provided if it's unreasonable for certain participants to attempt to satisfy the original standard because of a medical condition, or because it's medically inadvisable for them to try. A simple alternative is lowering the original standard. Plans can seek verification of a participant's medical condition from a doctor.

- Plan materials describing the wellness program and the monetary differentials must disclose the availability of the reasonable alternative standard. ❖