Health Reform
WK-EDGE

Wolters Kluwer

April 22, 2014

STRATEGIC PERSPECTIVES: Wellness programs: What employers need to know when it comes to HIPAA privacy and security rules

By Susan L. Smith, JD, MA

Wellness programs are designed to help employers manage their corporate health care costs by creating a healthier workforce. Wellness programs educate employees about health-related issues, promote the maintenance of healthy life styles, and encourage employees to make healthier choices, according to an article in the Wolters Kluwer Employee Relations Law Journal written by Catherine Livingston and Rick Bergstrom. As part of a wellness program, employers may ask employees to complete a health risk assessment or may offer free blood pressure screenings.

The Health Insurance Portability and Accountability Act (HIPAA) (P.L. 111-148) established the first rules for wellness programs by prohibiting group health plans from discriminating against individual participants and beneficiaries in eligibility, benefits or premiums based on health factors (nondiscrimination provisions) and more nondiscrimination rules were established for wellness programs that are group health plans by sec. 1201 of the Patient Protection and Affordable Care Act (ACA) (P.L. 111-148). An exception to the general rule allows premium discounts or rebates or modification to otherwise applicable cost sharing (including copayments, deductibles, or coinsurance) in return for adherence to certain programs of health promotion and disease prevention.

Because there has been little guidance offered by the government regarding other state and federal laws such as the Americans with Disabilities Act (ADA), Genetic Information Nondiscrimination (GINA) (P.L. 110-233), Employment Retirement Income Security Act (ERISA) (P.L. 93-406) as they apply to wellness programs, recent articles have been written addressing such laws. The implications of the HIPAA privacy and security rules for employers offering wellness programs, however, have not been addressed in depth recently. This Strategic Perspective discusses when and how the HIPAA privacy and security rules impact wellness programs and provides insight, recommendations, and suggestions from labor and employment law experts for employers to ensure that if the HIPAA privacy and security rules apply to them, they are in compliance with the requirements.

Statutory and regulatory provisions establishing wellness program rules

HIPAA generally prohibits group health plans from discriminating against participants and beneficiaries with respect to eligibility, benefits, and premiums or contributions based on certain specified health factors. Under HIPAA regulations, benefits must be offered uniformly to all similarly situated individuals but the regulations allow for benign discrimination in which individuals with adverse health factors are treated more favorably by employers, for example, by offering disease management programs. The HIPAA regulations created an exception to the nondiscriminatory requirement for wellness programs that meet certain requirements. This exception for wellness programs was addressed in the ACA, effective for plan or policy years begin on or after January 1, 2014. In addition to establishing categories for wellness programs, a maximum reward that could be offered was increased from 20 percent to 30 percent of the total cost of coverage and regulatory authority was granted for an increase up to 50 percent.

After the ACA was enacted, the Departments of Labor, Health and Human Services and Treasury adopted regulations (see 26 C.F.R. 54.9802-1(f)) clarifying the rules regarding the design of health-contingent wellness programs and the reasonable alternatives these programs must cover to avoid prohibited discrimination under the ACA, but questions remain regarding the implications of other laws such as the ADA, GINA, and ERISA, Livingston and Bergstrom said. The final rule was published in the *Federal Register* on June 3, 2013 (78 FR 33158), which set forth specific criteria that must be satisfied for group health promotion or disease prevention programs to qualify for an exception to the prohibition on discrimination based on health status, effective for plan or policy years beginning on or after January 1, 2014, changed the manner under which existing rules categorized wellness programs and expanded the requirement to offer a

reasonable alternative program for wellness programs that require the participant to meet a standard. The final rule established three wellness program categories:

Participatory

- Participatory wellness programs either do not provide a reward or do not include any conditions for obtaining a reward based on individuals satisfying a standard that is related to a health factor. A participatory wellness program offers a reward for participating without regard to the outcome. Examples of participatory wellness programs include a program that reimburses for all or part of the cost of membership in a fitness center; a diagnostic testing program that provides a reward for participation and does not base any part of the reward on outcomes, and a program that provides reward to employees for attending a monthly, no-cost health education seminar (*e.g.,* an employee who participates in a smoking cessation program receives a reward for participating without regard to whether the employee stops smoking).

Health Contingent Wellness Programs

Health-contingent wellness programs require an individual to satisfy a standard related to a health factor to obtain a reward. This standard may be performing or completing an activity related to a health factor or attaining or maintaining a specific health outcome. Health-contingent wellness programs are subdivided into (1) activity-only wellness programs, and (2) outcome-based wellness programs.

- **Activity only.** An activity-only wellness program requires an employee to perform or complete an activity such as a walking, diet, or exercise program that is related to a health factor to obtain a reward but do not require the individual to attain a specific health outcome. Some individuals may be unable to perform or complete an activity based on health status. Safeguards were included in the final rule to ensure these individuals are given a reasonable opportunity to qualify for the reward. The wellness program must meet certain requirements not to be considered impermissibly discriminate.

- **Outcome-based.** An outcome-based wellness program requires an individual to attain and/or maintain a specific measurable health outcome to obtain a reward, such as quitting smoking. An outcome-based wellness program will not be considered impermissibly discriminate if it meets similar requirements to the activity-only wellness program requirements but it must provide a reasonable alternative for an individual that does not meet the normal standard as well as those that have a medical issue that prevents them from meeting the standard. This program is considered health contingent. Examples of outcome-based wellness programs include a program that tests individuals for specified medical conditions or risk factors (such as high cholesterol, high blood pressure, or high glucose level) and provides a reward to employees identified as within a normal or healthy range, while requiring employees who are identified as outside the normal or healthy range to take additional steps (such as meeting with a health coach, taking a health or fitness course, adhering to a health improvement action plan, or complying with a health care provider's plan of care) to obtain the same reward.

Wellness Programs, 2014

Most companies view wellness programs as an essential part of their benefits program, according to an employer survey conducted by Fidelity Investments® and the National Business Group on Health (NBGH). The survey found that 95 percent of companies plan to offer some kind of health improvement program for their employees. In addition, the survey found that "the percentage of companies offering incentives to participate in these initiatives has increased from 57 percent in 2009 to 74 percent in 2014." Moreover, corporate employers plan to spend an average of $594 per employee on wellness-based incentives within their health care programs this year and an increasing number of companies are expanding wellness-based incentives to include spouses and domestic partners.

According to the survey, the most popular wellness programs target lifestyle management, such as physical activity programs, weight management programs, and stress management. Other popular health improvement options include disease/care management programs (*e.g.*, managing chronic health conditions, like diabetes), lifestyle-management services (*e.g.*, weight loss advice, gym membership discounts), health-risk management services (*e.g.*, on-site flu shots) and environmental enhancements (*e.g.*, bike racks, walking paths). While many employers offer incentives through cash or a gift card, an increasing number of employers offer incentives through an employer-sponsored health savings account (HSA), flexible spending account (FSA) or similar care-based savings vehicle, according to Fidelity news.

HIPAA Privacy and Security Rules and the Impact on the Implementation of Wellness Programs

According to wellness benefit administrators of a large global company, HIPAA privacy and security rules prevent them from getting information they need to incentivize employees participating in wellness programs. To better understand the issues Wellness benefit consultants encounter, Wolters Kluwer presented questions related to HIPAA privacy and security and wellness programs to three experts: Noelle Whitmire, JD, an associate at Jones Day, Atlanta, Georgia; Brian Clifford, Esq. an associate at Littler, Nashville Tennessee; and Andrea Bailey Powers, Esq., Of Counsel at Baker, Donelson, Bearman, Caldwell & Berkowitz, PC, Birmingham, Alabama.

How do HIPAA privacy and security rules impact employer Wellness Programs?

Whitmire: The HIPAA privacy and security rules apply to "health plans," which is a broadly defined term that includes an employee welfare benefit plan to the extent that the plan provides or pays for the diagnosis, cure, mitigation, treatment, or prevention of disease. The HIPAA privacy and security rules do not include provisions that are solely applicable to wellness programs nor are wellness programs exempted from the requirements of the HIPAA privacy and security rules. Thus, wellness programs that satisfy the definition of a "health plan" are subject to the HIPAA privacy and security requirements.

An employer-sponsored health plan may not disclose protected health information (PHI) to the employer for any employment-related actions or in connection with any nonhealth plan benefit of the employer. This rule applies to both a major medical health plan and a wellness program that is a health plan. Therefore, if the wellness program is a health plan (for example, a program targeted at preventing diabetes), information could be shared between the major medical plan and the wellness program. If the wellness program is not a health plan (for example, a walking club), however, then information may not be shared. There are additional hoops to jump through, such as providing proper notice, in sharing information as well as other laws, such as the GINA, that also must be considered, so sharing information should only be done after a careful analysis to ensure the rules are all met.

Clifford: Wellness programs are an exception to HIPAA's nondiscrimination provisions; not to its privacy and security rules. Protected health information (PHI) gained through a wellness plan is likely covered by HIPAA's privacy and security rules. Thus, the information must be protected from unauthorized disclosure by the health plan to the covered employer other than through permitted disclosures. For instance, covered employers may request summary, aggregate health information that results from a wellness program for the purpose of (i) obtaining premium bids from health plans for health insurance coverage under the health plan; (ii) modifying, amending, or terminating the group health plan; or (iii) when requested by the covered employer, to inform it whether an individual is participating in the group health plan or enrolled in or disenrolled from the health insurance offered by the plan. Otherwise, the PHI gained through the wellness program must be protected pursuant to HIPAA's privacy and security rules.

The wellness program will likely come under the HIPAA privacy rules if it is a term of an employee benefit program covered by HIPAA. If the program does not provide health care, but is employment based, then it may not be covered by HIPAA. This is rarely, if ever, the case, and a wellness program that is not a part of a bona fide employee benefit plan risks violating the ADA. Also, note that if the consultants sign a HIPAA-compliant Business Associate Agreement (BAA) and restrict the uses and disclosures of any PHI as limited in the BAA, this should not be a violation of HIPAA. Wellness Benefit Consultants should know this.

What do employers find most difficult in ensuring that an employee's protected health information is secure?

Clifford: It's important to note that the group health plan is the covered entity, not the employer in its role as such. The employer is a covered entity only in its role as a plan administrator of the group health plan. In my experience, the smaller the employer, the more difficult it becomes to separate out its role as plan administrator from its role as employer because it does not have the luxury of employees in specialized roles. Even so, some employers are unsure whether they are even covered by HIPAA's privacy and security rules. If they are covered entities, many employers have trouble determining what information is PHI, who may maintain the information, how they are to maintain it, and what information and to whom they may disclose it. Then they must develop and implement appropriate policies and procedures to ensure compliance with HIPAA's privacy and security rules. This is not an easy task for any employer; but it is necessary.

Powers: Understanding what the law requires and what it does not. […] Employers often get confused about the HIPAA rules that apply to health information and don't realize that only that information that flows through the health plan is covered by HIPAA privacy rules. While there may be other privacy laws that require [health information] be kept confidential, medical information provided for FMLA purposes is not covered by HIPAA. Other issues that can arise with HIPAA privacy relate to the sharing of health information. Employers need to be reminded that [properly] redacted or "de-identified" health information can be shared without violating the [HIPAA] privacy rule. This information is often needed in business acquisitions where the purchasing company requests claims information for purposes of assessing health plan costs.

Dusty files are another problem. When the HIPAA privacy rule was first implemented […] many health plan sponsors prepared the necessary HIPAA privacy compliance materials and underwent training. It is not unusual to find employers that have not touched the compliance materials or done any updated training since. There have been significant changes in the privacy rule […] since 2003 and as health plan sponsors, employers need to assure that their HIPAA privacy policies and procedures are current and that all those employees with access to PHI are properly trained.

In terms of wellness programs that require participating employees to undergo a biometric screening and complete a health risk assessment, how do employers ensure only authorized employees have access to the information and meet disclosure rules?

Whitmire: The HIPAA privacy rule applies to "PHI," which is any health information that is created for or received by a health plan; relates to the past, present, or future physical or mental health condition of an individual, or to the past, present, or future payment for an individual's health care; identifies the individual or if there is a reasonable basis to believe the information can be used to identify the individual; and is transmitted or maintained in any format (including oral, written, and electronic communications). Under the HIPAA privacy rule, the determination of whether information is "PHI" is not based on the sensitivity of the information. This means that the results of biometric screenings and health risk assessments are "PHI" in the same manner as other individually identifiable information maintained by the health plan, such as a claim for benefits, a participant's elections for health plan coverage, or the amount of a participant's premium.

The HIPAA privacy rule requires that health plans ensure adequate separation between the health plan and its plan sponsor and to make sure that the use and disclosure of PHI is limited to certain narrow purposes. Only certain employees may have access to PHI, and their access is restricted to necessary plan administration function. Further, there must be a process to correct and prevent recurrences of noncompliance with the HIPAA privacy and security rules. The HIPAA privacy rule also requires health plans to implement administrative, technical, and physical safeguards to protect the privacy of PHI. Typical procedures for implementing this requirement include: (1) requiring employees to keep PHI in a locked drawer or a locked cabinet when it is not being used or when the employee is away from his or her desk for an extended period; (2) destroying or shredding PHI when it is no longer needed; (3) storing documents that contain PHI in a secure location with access limited to authorized employees; (4) instructing employees who have access to PHI to close their doors when discussing PHI; (5) using dedicated fax and copy machines for areas in which PHI is used; and (6) making sure that the address is correct if PHI is mailed.

Clifford: Employers with fully insured plans generally need not worry about accessing PHI resulting from a wellness program because their insurer collects the information and administers the plan. On the other hand, employers with self-insured plans must ensure that the health plan collects the information and maintains it except for permitted disclosures to the covered employer. Employers with self-insured plans that also self-administer the plan must ensure that PHI stays with designated and authorized employees. Even here, however, the administration of the wellness program should be delegated to a third party provider that has executed a BAA. In any event, a covered employer is required to develop and implement policies and procedures that comply with HIPAA privacy and security rules. Then the covered employer must ensure adequate separation between the employer and the health plan collecting PHI related to a proper wellness program. Essentially, the HIPAA privacy policy should:

- describe those employees or classes of employees under the control of the employer/sponsor that are given access to PHI;
- restrict the access to and use of PHI to those employees described above; and
- provide an effective mechanism for resolving any issues of noncompliance by those employees described above.

The covered employer must train the designated employees on HIPAA's privacy and security rules and how to comply with them. When these efforts are done correctly, covered employers can greatly reduce the risk of disclosing protected health information.

Powers: Employers need to train personnel on privacy requirements, assure physical security of PHI, and verify all electronic PHI meets privacy standards, including HITECH Act requirements. While employers may do all of this, some employees may still be uncomfortable that a colleague -- even a very well trained colleague -- will have access to their very private health information. To reassure employees and also to reduce exposure for a HIPAA privacy violation, some employers may engage third parties to perform the health risk assessments and manage their wellness program. These third party vendors can assure that employers see only summary results and that no PHI is shared with the employers. Companies looking to utilize third party vendors for wellness program management should carefully review the vendor's capabilities, obtain appropriate business associate agreements and check the vendor's references.

Do employers generally have policies and procedures in place to prevent and address breaches of data and, in your experience, how large of a problem is the possibility of a breach of the data gathered from employees who participate in employers' wellness programs?

Whitmire: Both the HIPAA privacy and security rules require health plans to have written policies and procedures in place to ensure compliance with the rules. In the event of any acquisition, access, use, or disclosure of PHI in a manner that is not permitted by the privacy rule, the health plan must either (a) conduct a risk assessment to demonstrate that there is a low probability that the PHI has been compromised; or (b) treat the incident as a "breach" of PHI. A "breach" is a defined term under HIPAA and generally means any acquisition, access, use, or disclosure of PHI in a manner that is not permitted under the HIPAA privacy rule that compromises the security or privacy of PHI. […] We have not seen that wellness programs are any more susceptible to breaches than any other type of health plan, and we have not found breaches to be prevalent with respect to health plans. If there is a breach, it frequently involves a theft of a desktop computer or mobile device.

Powers: HIPAA requires that there be policies and procedures in place. Often these are well out of date and not reviewed with any regularity, as noted above. Employers need to address privacy issues on a routine basis and work with their advisors to assure security of the information.

What steps do you recommend employers to take to ensure they are in compliance with HIPAA privacy and security rules when a wellness program requires collection of protected health information?

Whitmire: If an employer is already complying with HIPAA's privacy and security requirements with respect to its existing health plans, there are no additional requirements if it decides to implement a wellness program, other than ensuring that the existing HIPAA policies and procedures apply to the wellness program's PHI. If the employer is using an outside vendor to implement the wellness program, the health plan will need to determine whether a business associate agreement is required with the vendor.

Clifford: Ensuring HIPAA compliance is no easy task, especially for employers who are unfamiliar with HIPAA requirements. Employers who have implemented a new wellness program or are thinking about doing so should seek counsel to ensure their HIPAA strategy and compliant policies will pass muster and prevent disclosure of protected health information. Wellness programs are always, at least should be – unless the employer is also a health provider - administered by a third party provider or the health insurer. There should always be a HIPAA-compliant BAA with the party filling this role. That agreement should have strong protections and remedies for the employer in case of any breach. Generally, a covered employer is required to develop and implement policies and procedures pursuant to HIPAA privacy and security rules. Then the covered employers must designate certain employees that will have access to protected health information, train those employees on HIPAA privacy and security rules, train them on how to comply with the employer's HIPAA policies and procedures, and provide a mechanism for resolving issues of noncompliance.

What steps do employers take to ensure that mobile devices are secure (laptops and phones)?

Whitmire: Typical steps that employers take to protect PHI on mobile devices include: (1) requiring password protection on mobile devices and any documents containing PHI; (2) using programs to remotely delete information from missing or stolen devices; (3) instructing employees to never leave mobile devices unattended; and (4) instructing employees to delete PHI from the device when the information is no longer needed.

Clifford: First, allowing mobile access to PHI is almost always an unnecessary risk. Mobile devices such as laptops, tablets, and smart phones are particularly vulnerable to a breach of HIPAA privacy and security rules because of their ability to take PHI outside the four walls of the employer. Employers should take extreme precautions when allowing offsite access to employees' PHI and should do so only when such offsite access is an absolute necessity. If employers allow the use of mobile devices to access or store PHI, HIPAA regulations requires them to implement policies and procedures to prevent unauthorized disclosure of PHI from those devices. Employers also should establish risk management strategies to safeguard such information on mobile devices. For example, risk management strategies may include the following:

- identify the data hardware that must be tracked;
- keep a record of the person(s) authorized to access PHI and those permitted mobile access to such information;
- require automatic time-outs and lock codes on those mobile devices;
- password protect files;
- encrypt the data on those mobile devices; and
- ensure appropriate security updates are installed on the mobile devices.

Conclusion

According to Clifford, to the extent the employer is a covered entity, it is required by HIPAA to adopt a HIPAA privacy and security policy, to appoint a privacy and security officer, provide all affected individuals with a notice of privacy rights, usually in the health plan's [summary plan description] SPD, and to train all persons who will have access to PHI. Rarely do employers that understand they are covered fail to develop some form of HIPAA policy. Safeguarding against nondisclosure of PHI gained through wellness programs really is no different than safeguarding PHI gained through other means. Problems typically arise, however, when you have an employer who implements a new wellness program and is unfamiliar with its obligations under HIPAA.

Attorneys: Noelle Whitmire (Jones Day), Brian Clifford (Littler), Andrea Bailey Powers (Baker, Donelson, Bearman, Caldwell & Berkowitz, PC)

MainStory: StrategicPerspectives NewsFeed PreventiveNews