



education | research | information

benefits

MAGAZINE

Reproduced with permission from *Benefits Magazine*, Volume 55, No. 1, January 2018, pages 34-38, published by the International Foundation of Employee Benefit Plans (www.ifebp.org), Brookfield, Wis. All rights reserved. Statements or opinions expressed in this article are those of the author and do not necessarily represent the views or positions of the International Foundation, its officers, directors or staff. No further transmission or electronic distribution of this material is permitted.

PRIVACY CONSIDERATIONS FOR EMPLOYER- SPONSORED WELLNESS PROGRAMS

Employers must be mindful of their duty to protect the privacy of the health information employees may share when participating in a workplace wellness program.

Given the highly sensitive nature of medical data collected in connection with wellness programs, the privacy and security of such information should be of utmost importance to plan sponsors and participants alike. Unauthorized disclosure of participants' health information can lead to a range of consequences—from potential embarrassment to breach-of-privacy claims to investigations by the U.S. Department of Health and Human Services.

While specific breach-of-privacy laws may vary from state to state, federal laws, including the Americans with Disabilities Act (ADA) and the Genetic Information Nondisclosure Act of 2008 (GINA), recognize the significant privacy implications involved in employer requests for medical information about their employees. Employers are typically prohibited under ADA and GINA from collecting health care information about their employees, but both of those laws carve out exceptions in the context of wellness programs. When implementing wellness programs, plan sponsors should take steps to carefully comply with these and other applicable laws and regulations in order to mitigate potential liability.

Risks to Participants

Individuals typically view their medical information as highly sensitive, and the thought of it being shared with their employer may be enough to prevent employees from participating in employer-sponsored wellness programs from the outset. While employees may expect their own health care providers to carefully safeguard their medical information, often it is less clear precisely how their information may be protected when shared in the context of an employer-sponsored wellness program. Plan participants are rightly concerned about the steps plan sponsors are taking to protect their medical information from improper disclosure, as well as the types of disclosures that are (and are not) permitted under the law.

When plan sponsors fail to appropriately safeguard medical information shared as part of a wellness program, participants risk having their protected health information (PHI) shared with their supervisor and used against them in employment-related decisions or even having that information shared publicly. For example, PHI may include medical diagnoses, treatment history or other sensitive medical information. In addition, participants potentially risk having their medical identities stolen, whereby thieves may use information such as a name, Social Security number or Medicare number to buy drugs, obtain health care or submit fake billings to a health insurer in the participant's name. Medical identity theft can be disruptive, damaging and potentially life-threatening if thieves cause misinformation to be incorporated into medical records.

learn more

Education

To watch Kristen Whittle's recorded webcast presentation, "**Employee Wellness Challenges: Keeping Them Well, Keeping You Compliant**," visit www.ifebp.org/webcasts.

From the Bookstore

Rule the Rules of Workplace Wellness Programs

Barbara J. Zabawa, J.D., M.P.H., and Joann M. Eickhoff-Shemek, Ph.D. American Bar Association. 2017.

Visit www.ifebp.org/books.asp?9106 for more information.

Workplace Wellness That Works

Laura Putnam. Wiley. 2015.

Visit www.ifebp.org/books.asp?9058 for more details.

Risks to Plan Sponsors

In addition to the risks to its participants, a plan sponsor's failure to appropriately protect medical information obtained in the context of a wellness program may lead to liability and other consequences. Employees may be unwilling to participate in a wellness program that they view as unsecure—thus dooming the wellness program for failure before it begins. Once underway, a wellness program that subsequently discloses participant medical information may find it leads to immediate internal consequences such as morale issues and employee turnover. Thereafter, participants whose PHI has been disclosed to a third party may seek to recover for any related damages by filing a lawsuit against the plan sponsor under applicable state law breach-of-privacy statutes. Moreover, health plans that are subject to the Health Insurance Portability and Accountability Act (HIPAA) requirements may risk investigations and enforcement actions by the Department of Health and Human Services (HHS) arising out of a failure to safeguard medical information. Accordingly, plan sponsors should be aware of the applicable legal requirements and should continually evaluate their wellness programs for compliance.

Requirements for Safeguarding Medical Information

Employers are required to maintain the privacy and security of employees' personally identifiable health information collected in the context of employer-sponsored wellness programs. Specifically, employers must safeguard any information about a particular individual relating to his or her medical condition or history. While plan sponsors may use aggregate information to tailor wellness programs to specific health risks identified in a particular workplace, employers may not use personally identifiable health information for employment-related decisions—except in order to respond to an employee's request for a reasonable accommodation under ADA. For example, employers may use information demonstrating that many participants experience high cholesterol in the context of implementing specific aspects of a wellness program but cannot discipline an individual employee on the basis of his or her high cholesterol.

Moreover, employers may not require an employee to agree to the sale, transfer or other disclosure of PHI or to waive confidentiality protections under applicable law as a condition for participating in a wellness program or receiv-

ing an incentive for participating, except to the extent necessary to carry out specific, permissible activities related to the wellness program. Employers must then keep the PHI confidential and limited to the context of the wellness program. When implementing a wellness program, employers should specify the individuals who will receive PHI, such as a medical professional or health coach, in order to provide services within the scope of the program.

Where wellness programs involve the collection of genetic information, GINA applies to impose additional specific requirements, which were recently clarified with guidance from the Equal Employment Opportunity Commission in 2016.

Specifically, GINA requires employers to obtain an authorization from plan participants before collecting genetic information as part of an employer-sponsored wellness program. The authorization must explain the restrictions on the disclosure of that information, that individually identifiable genetic information is given only to the health care professionals involved in providing services and that any individually identifiable genetic information is obtained only for purposes of participation in the wellness program and shall not be disclosed to the employer except in aggregate terms.

Similarly, new rules under ADA require employers offering wellness programs that collect employee health information to provide a notice to employees informing them what information will be collected, how it will be used, who will receive it and what will be done to keep it confidential. This full-disclosure requirement is intended to ensure that participants are fully

aware of the scope of medical information to be collected before such information is actually disclosed.

Under GINA, employers and other entities that possess genetic information must maintain it in a medical file (whether paper or electronic) that is separate from an employee's medical file. The employer must protect that information as a confidential medical record.

Under the framework of both ADA and GINA, in order to mitigate potential discrimination claims, employers should never commingle medical/genetic information related to wellness programs with personnel files. Rather, any information related to employee participation in a wellness program should be kept in a separate, secure location. In addition, an employee's participation or nonparticipation in a wellness program should not factor into other employment-related decisions. To the extent possible, employee health-related information should not be shared with supervisors in order to avoid any possibility that such informa-

tion could be used in a discriminatory manner.

The segregation of medical and genetic information obtained in the context of a wellness program from employee personnel files should help employers ward off potential discrimination claims and also may encourage employees to freely share information with a wellness program without fear of repercussions from the employer. For example, an employee who is trying to become pregnant may be less likely to disclose that information in the context of an employer-sponsored wellness program if she had a concern that her supervisor might find out. Accordingly, strict compliance with ADA and GINA may ultimately promote the efficacy of wellness programs as well as reduce potential liability.

HIPAA Concerns

Where workplace wellness programs are offered as part of a group health plan, the HIPAA Privacy Rule imposes additional requirements to those imposed by ADA and GINA. Importantly,

takeaways

- Federal laws, including the Americans with Disabilities Act (ADA), Genetic Information Nondisclosure Act of 2008 (GINA) and the Health Insurance Portability and Accessibility Act (HIPAA), have requirements dealing with the collection of employee health information that affect wellness programs.
- Wellness program sponsors that fail to protect employee medical information face a range of risks from lack of participation in the program to lawsuits and federal enforcement actions.
- Under ADA, employers cannot ask or require employees to waive the confidentiality of their protected health information (PHI) as a condition of participating in a wellness program.
- GINA requires employers to obtain an authorization from plan participants before collecting genetic information for a wellness program.
- Segregating employee medical information from personnel files should help protect employers from potential discrimination claims.

HIPAA applies only to *covered entities*, including (1) health plans, (2) health care clearinghouses and (3) health care providers that electronically transmit any health information—but not to employers acting in their capacity as employers. Accordingly, wellness programs that are offered in connection with an employer-sponsored group health insurance plan would be subject to stringent HIPAA requirements, but employers that create their own wellness plans using internal resources without relation to a group health insurance plan would not. As a best practice, however, employer-sponsored wellness programs that are not subject to HIPAA may nonetheless choose to follow its guidelines.

Under HIPAA, PHI may not be disclosed except in limited circumstances. The HIPAA Privacy Rule protects most “individually identifiable health information”—also known as PHI—that is maintained or transmitted by a covered entity or its business associate, in any form, whether electronic, on paper or oral. The HHS Office of Civil Rights (OCR) enforces HIPAA requirements. According to data released in August 2017, OCR had received more than 163,277 HIPAA complaints and has initiated more than 847 compliance reviews since the implementation of the HIPAA Privacy Rule in 2003. OCR required covered entities to implement correc-

tive action in 69% of all resolved investigations during that time frame.

When employers implement a wellness program as part of a group health plan, the employer and the group health plan should mutually certify that they will each safeguard the PHI disclosed as part of the wellness plan and not improperly use or share the information. Group health plans also should require the execution of business associate agreements with vendors who may receive PHI in order to implement the wellness program, as needed.

Select Vendors Carefully

When working with a wellness program vendor, particularly one unconnected with a group health insurance plan, employers should ensure that the vendor utilizes industry-standard or industry-leading techniques for protecting the privacy of health information. Vendors are not subject to the same HIPAA requirements imposed on group health insurance plans and are technically not prohibited from selling or otherwise using highly sensitive medical information obtained in the context of a wellness program. Thus, plan participants risk having their health information sold without their consent, potentially also leading to legal liability for the employer.

Accordingly, even where HIPAA does not technically apply, employers should ensure that the vendor assumes similar responsibilities and obligations imposed by its Privacy Rule as a best practice. In such a vendor agreement, employers should consider including indemnity provisions for legal protection in the event that a vendor fails to comply with its obligations in this regard.

Conclusion

Careful planning before implementing a wellness program can go a long way in mitigating risks. Once a wellness program is underway, plan sponsors should regularly audit the program for compliance and make adjustments as necessary. While it is nearly impossible to completely avoid the risk of liability, careful compliance with applicable requirements can provide a solid defense in the event of a claim. ❶

bio



Kristen M. Whittle is a partner at Barton Gilman LLP, a litigation firm with offices in Boston, Massachusetts; Providence, Rhode Island; and New York, New York.

She regularly advises employers on all aspects of the employment relationship—from hiring through separation—and she frequently reviews and revises personnel policies and handbooks. She devotes a significant portion of her practice to assisting clients in the nonprofit and small business communities. Whittle obtained her undergraduate degree from Boston College and her law degree from Boston College Law School.

