November/December 2016 Newsletter
By Barbara J. Zabawa, JD, MPH
Center for Health and Wellness Law, LLC

The EEOC Rules and Your Wellness Portal

Many workplace wellness programs use a wellness portal that participants use to provide health information through a health risk assessment, learn healthy living tips, track fitness or nutrition progress, among other things. These wellness portals are not immune from complying with laws governing the collection, storage, use and disclosure of participant health information. Owners of wellness portals must be aware of requirements under HIPAA, the FTC Act, the Americans with Disabilities Act (ADA) and the Genetic Information Nondiscrimination Act (GINA), for example.

In May 2016, the Equal Employment Opportunity Commission (EEOC) issued final rules under the ADA and GINA that impact wellness portals. The ADA requires wellness programs that collect health information, regardless of whether there are any incentives, to provide participants with a notice. The notice must be understandable, describe the type of medical information that will be obtained, the specific purposes for which the information will be used, and describe how the employer will protect that health information from improper disclosure. The EEOC issued a sample notice, which can be found here. Importantly, this notice must be provided ***before*** the participant reveals their health information through the portal. That means that the portal must have a mechanism in place to ensure that the participant sees the notice. This might be through a pop-up window that the participant must read before moving into the portal services and offerings.

Similarly, the GINA rules require an "authorization" for the collection of "genetic information." The final GINA rules now permit wellness programs to incentivize employee spouses to disclose the spouse's manifestation of disease or disorder information. Such information is considered "genetic information" and may be collected through a spouse completing a health risk assessment on the wellness portal. Before the spouse can disclose that information, however, the spouse must provide "prior, knowing, voluntary and written authorization." The authorization form must also describe the confidentiality protections and restrictions on the disclosure of genetic information.

For wellness portals, this prior, knowing, voluntary and written authorization may need to take the form of a pop-up window that the wellness participant actively acknowledges seeing and reading, perhaps through an electronic signature, before revealing their manifestation of disease or disorder information through the portal. The Center for Health and Wellness Law, LLC has helped clients navigate how to address these requirements through wellness portals.

One other item of note for wellness portals under the EEOC rules: portals should not just be about collecting health information. The portal must offer meaningful follow-up to the participants in order to meet the ADA and GINA requirements that the wellness program be

"reasonably designed to promote health and prevent disease." The EEOC rules state that the program must provide results, follow-up information or advice in order to be reasonably designed to promote health or prevent disease. The Center for Health and Wellness Law, LLC can help ensure your portal is in compliance. Please contact our firm to assist with your wellness compliance needs.

Does it Matter How and When You Provide the ADA and GINA Notice/Authorization?

"Yes." The GINA authorization requirement is easy to explain – the authorization must be "***prior***, written and knowing," so it must occur **before** an individual discloses their "genetic information." Thus, if your wellness program incentivizes spouses to participate in a health assessment or biometric screen, or if your HRA asks employees family medical history questions, the employer should be obtaining the spouse or employee's authorization before they divulge their genetic information.

The ADA's new notice requirement should also be occurring **before** the wellness program gathers the wellness participant's genetic information. Even though the regulations do not specify that the notice has to "prior and knowing," the ADA regulations do specify that the wellness program must be "voluntary." The preamble to the final rule states that "For these wellness programs [that conduct disability-related inquiries and/or conduct medical examinations] to be deemed voluntary, a covered entity must provide a notice – in language reasonably likely to be understood by the employee from whom medical information is being obtained = that clearly explains what medical information will be obtained, how the medical information will be used, who will receive the medical information, the restrictions on disclosure, and the methods the covered entity uses to prevent improper disclosure of medical information. 81 Fed. Reg. at 31134 (May 17, 2016). Failing to ensure that employees read the notice before supplying their health information would undermine the voluntary nature of disclosing their health information.

Also, and perhaps more directly, the EEOC in its Questions and Answers document states that employees must receive the notice before providing any health information, and with enough time to decide whether to participate in the program. "Waiting until after an employee has completed an HRA or medical examination to provide the notice is illegal."

Why do I emphasize the timing of delivery of the notice? Because some employers and/or wellness vendors may be providing the notice on their website as a link, but not creating a mechanism to ensure that employees are reading the notice before they provide health information. As stated by the EEOC, failing to ensure that employees are reading the notice before divulging their health information is illegal. As a result, it is very important that the timing of your notice meets EEOC expectations.

What are the penalties for failing to abide by the notice rules? Failure to comply with the ADA and GINA notice/authorization requirements can result in Civil Monetary Penalties

to the employer in the amount of $525 per violation. That means for every individual who does not receive the notice/authorization that should have received it, the employer would face a penalty of $525 per person. This could amount to a lot of money very quickly. Here is a link to 29 CFR 1601.30 that discusses the penalties for noncompliance with ADA and GINA notice requirements: https://www.law.cornell.edu/cfr/text/29/1601.30.

As always, please consider the Center for Health and Wellness Law, LLC a resource in helping you comply with the notice and authorization requirements.

Do the HIPAA Privacy and Security Rules Apply to Workplace Wellness Programs?

I get this question very often, and the answer is, "it depends." Specifically, it depends on whether the wellness program is part of an employer's group health plan, or if it is a stand-alone program offered directly by the employer. Many providers of wellness services contract with group health plans as well as employers directly, which means some wellness programs are offered to group health plan participants only, and others are offered to all employees, regardless of the employee's health insurance status.

For programs that are offered by group health plans to group health plan participants only, the answer to the HIPAA privacy and security question is an unequivocal "yes." Group health plans are one type of "covered entity' under the HIPAA privacy and security rules. Therefore, any wellness provider who contracts with those health plans must comply with HIPAA privacy and security as a "business associate."

For wellness programs that are offered to all employees, however, HIPAA privacy and security rules likely do not apply. The federal Department of Health and Human Services (HHS) recently released subregulatory guidance about when and how HIPAA privacy and security rules apply to workplace wellness programs. HHS concludes that HIPAA privacy and security rules apply to workplace wellness programs when those programs are part of a group health plan for employees. The wellness vendor in that situation would be a "business associate" of the group health plan "covered entity" under HIPAA. As a result, the wellness vendor would need to comply with the HIPAA security rule, have a HIPAA-compliant business associate agreement, and have policies and procedures in place for issues like data breaches.

Wellness programs that are offered by employers directly and not as part of a group health plan are not subject to HIPAA privacy and security rules. However, other federal or state laws may apply and regulate the collection and/or use of employee health information.

Even if HIPAA Privacy & Security Do Not Apply, It May Be a Good Idea to Comply

Anyway.

Some wellness programs decide to comply with HIPAA privacy and security rules even when those rules do not technically apply to them. If a wellness program collects sensitive health information from employees and family members, it may be a good idea to adopt HIPAA security privacy and security standards to help protect the information from unauthorized use and disclosure.

Indeed, in July 2016, HHS released a Fact Sheet regarding ransomware. Ransomware is a type of malicious software that denies access to a user's data, usually by encrypting the data with a key known only to the hacker who deployed the software, until a ransom is paid. Ransomware attacks are skyrocketing, particularly on health and wellness organizations. According to HHS, there was a 300% increase in ransomware attacks between 2015 and 2016. Health information is more valuable than other types of personal information. According to one source, health record information is ten times more valuable than credit card information. This is because credit card information is insured, while health information has less protection.

HHS states that HIPAA compliance can help entities prevent infections of malicious software, including ransomware. HIPAA security rules require entities to take the following actions that could prevent a ransomware attack:

- Implement a security management process, including a risk analysis to identify threats and vulnerabilities to health information;
- Implement security measures to mitigate or remediate those risks;
- Train users on malicious software protection so they can assist in detecting malicious software and know how to report such detections; and
- Implement access controls to limit access to electronic health information to only those persons or software programs requiring access.

As a result, if your wellness program collects health information, regardless of whether you are subject to HIPAA privacy and security rules, it may be prudent to comply with those rules anyway. Compliance can help safeguard your wellness program from a ransomware or other type of unauthorized use and disclosure. It can also give wellness program clients and participants confidence in how you handle health data.

For assistance with meeting HIPAA privacy and security standards, contact the Center for Health and Wellness Law, LLC.

Just in Time for the Holidays: OIG Increases Amount of "Nominal" Gifts Permitted under the Anti-Kickback Statute

If you are a health care provider who serves Medicare, Medicaid or Veterans' benefits patients, you may wonder whether you can offer a gift to your patients, particularly

around the holidays. You may want to give the gift as a "thank you" for their patronage. However, the federal anti-kickback statute (AKS) usually prohibits offering federally-funded patients anything of value, as such a gift might induce those patients to see you more and therefore increase federal health care expenses.

The federal Office of Inspector General (OIG), issued a Policy Statement on December 7, 2016, stating that gifts of "nominal" value are permissible and won't violate the AKS. OIG has increased the nominal value to $15 per item or $75 in the aggregate per patient on an annual basis. The gift may NOT be cash or cash equivalents, however. Thus, gift cards are out. But, if a provider wanted to give a patient a material item one time a year whose value was no more than $75, that would be permissible. The nominal value had not been increased since 2000.

If you have any questions about AKS compliance or giving gifts to patients, please contact the Center for Health and Wellness Law, LLC for help.

Federal Health and Human Services Lists All Recent and Pending Regulations

If you are curious to know what regulations the federal Department of Health and Human Services (HHS) has released this year or still intending to release in the near future, you now have a resource. HHS recently issued a list of all of its recent and pending rules, and the stage of those rules. This list includes rules that affect Medicare, Medicaid, mental health records, CDC, FDA, health research, among others. To view the list, click here.

21st Century Cures Act Cuts ACA Prevention Funding, Supports Efforts in Other Health Areas

The 21st Century Cures Act, passed by Congress on December 7, 2016, is a "grab bag of goodies," as one source called it. But, it also decimates much of the prevention funding provided by the Affordable Care Act by cutting $3.5 billion over 10 years from the Prevention and Public Health Fund. According to Modern Healthcare, that fund helped battle Alzheimer's disease, smoking, lead poisoning, heart disease, diabetes, stroke and falls among elderly adults. The fund also served as a resource for programs that promote breastfeeding, enable self-management among those living with chronic disease, improve tracking of hospital-acquired infections, address racial health disparities and increase immunization. This cut will especially impact the Centers for Disease Control.

Trust for America's Health is asking for support in signing a letter to Congressional leadership opposing the repeal of the Prevention and Public Health Fund.

In exchange for cutting prevention dollars, the 21st Century Cures Act allocates more funding to fighting opioid addiction, drugs and medical device innovation, cancer

research, facilitates interoperability and leverage of electronic health records, improves States' ability to detect health care providers who have been terminated from the Medicare program, allocates money and other resources to improve mental health and substance use disorder care (including enhancing compliance with mental health parity laws), changes reimbursement for hospital outpatient departments, among other items.

The Cures Act also allows small employers (those with fewer than 50 employees) to offer employees a pre-tax Health Reimbursement Account to help employees pay for individual health insurance premiums on the individual insurance market. That is, starting January 1, 2017, small employers can deposit money into an account, pre-tax, that employees can use to pay for individual health insurance. Before the Cures Act, no employer could offer this benefit without also offering comprehensive health benefits that met Affordable Care Act standards. Now, employers who don't offer health insurance can at least offer their employees some financial help in affording individual health insurance.

To see a summary of all the provisions of the Cures Act, click here.

Register Now for the 2017 WELCOA Summit and Pre-Conference, August 28-30th in Omaha, NE!

Barbara Zabawa, JD, MPH from the Center for Health and Wellness Law, LLC will be conducting a pre-conference session on Wellness Compliance. See the full agenda and information on how to register, here.

Are You a WELCOA Member? Sign Up for My Monthly Legal Update Webinars Starting January 2017!

The Center for Health and Wellness Law, LLC has teamed up with WELCOA to offer WELCOA members monthly legal update webinars. Each month the webinars will explore a different wellness compliance issue, leaving plenty of time for questions and answers to wellness compliance questions from attendees. Don't miss this great opportunity to stay on top of wellness compliance issues! You can learn more and register here.

For more articles, please see our blog page.