OCR Addresses Application of HIPAA Privacy Rule to Workplace Wellness Programs

R. Michael Barry

Healthcare providers are accustomed to the privacy and security rules contained within the Health Insurance Portability and Accountability Act ("HIPAA" or the "Act") – particularly as they apply to the careful management of patient information. On April 24, 2015, the Health and Human Services Office for Civil Rights (OCR) issued important guidance regarding HIPAA's application to employee health and wellness programs. OCR is responsible for enforcing the Act's privacy and security rules.

The HIPAA privacy and security rules generally apply to "covered entities" – defined as (1) A health plan; (2) A health care clearinghouse; or (3) A health care provider who transmits any health information in electronic. The rules also apply to "business associates." The Act is most often associated with medical records generated by a health care provider. An employer – solely by hiring and paying an employee – is not impacted by the obligations of the Act. In general, the Act does not apply to an employee's employment records.

OCR's recent guidance addresses two important issues: 1) when does the Act extend to an employer's health and wellness program; and 2) when may a health plan provide a sponsor employer with access to a participant's protected health information (PHI).

The recent guidance makes clear that the application of the Act depends upon the structure of the employer's health and wellness plan. Note that a health plan is a "covered entity" and is subject to the Act. OCR noted that a health and wellness program that is offered to employees as part of the employer's health plan benefit is covered by the Act and its rules. A health and wellness program that is not part of a health plan is not covered by the Act and its rules – though other federal and state laws may apply to protect the confidential nature of such information.

In many instances, an employer (as the health plan's sponsor) may administer the health and wellness program (among other elements of the plan). A health plan (a "covered entity" and subject to the Act) may provide an employer-sponsor access to an employee's health information under limited circumstances where the employer-sponsor is involved in administering the program. In particular, the employer-sponsor may provide access to the employee's PHI only to permit the employer-sponsor to perform its administrative functions and agree to modify its plan documents and certify that it will:[1]

1. Establish adequate separation between employees who perform plan administration functions and those who do not;
2. Not use or disclose PHI for employment-related actions or other purposes not permitted by the Privacy Rule;
3. Where electronic PHI is involved, implement reasonable and appropriate administrative, technical, and physical safeguards to protect the information, including by ensuring that there are firewalls or other security measures in place to support the required separation between plan administration and employment functions; and report to the group health plan any unauthorized use or disclosure, or other security incident, of which it becomes aware.

Health plans and employers (particularly those within the health care industry where HIPAA

1 See 45 C.F.R. § § 164.314(b) and 164.504(f)(1)(i) and (f)(2).

awareness is already high) should be prepared to proactively address the protection of and access afforded to an employee-participants' PHI. In addition, since the health plan (as a "covered entity") has specific obligations related to any PHI breach, health plan and employer-sponsor should carefully and thoroughly review the privacy and security protection provided to all employee-participant PHI.

If an employee-sponsor does not perform administrative functions on behalf of the health plan, access to an employee-participant's PHI is further limited. In particular, in such instances, the health plan may only disclose: 1) information on which individuals are participating in the plan or enrolled in the health insurance issuer or HMO offered by the plan; and 2) summary health information to the extent requested for purposes of modifying the plan or obtaining premium bids for coverage under the plan.

For more information regarding OCR's application of the HIPAA Privacy Rule to Workplace Wellness Programs, see, http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/wellness/index.html (accessed April 27, 2015).

Authors and Contributors

R. Michael Barry
Partner, Atlanta Office
404.873.8698
michael.barry@agg.com

not *if*, but *how*.®

About Arnall Golden Gregory LLP

Arnall Golden Gregory, a law firm with more than 150 attorneys in Atlanta and Washington, DC, employs a "business sensibility" approach, developing a deep understanding of each client's industry and situation in order to find a customized, cost-sensitive solution, and then continuing to help them stay one step ahead. Selected for The National Law Journal's prestigious 2013 Midsize Hot List, the firm offers corporate, litigation and regulatory services for numerous industries, including healthcare, life sciences, global logistics and transportation, real estate, food distribution, financial services, franchising, consumer products and services, information services, energy and manufacturing. AGG subscribes to the belief "not if, but how.®" Visit www.agg.com.

Atlanta Office
171 17th Street, NW
Suite 2100
Atlanta, GA 30363

Washington, DC Office
1775 Pennsylvania Avenue, NW
Suite 1000
Washington, DC 20006

To subscribe to future alerts, insights and newsletters: **http://www.agg.com/subscribe/**