PRIVACY ALERT
December 30, 2013

Wellness Subcontractor's Breach Leads to Office for Civil Rights Complaint

Class Action Lawsuit Also Possible

The City of Milwaukee filed a complaint with the Department of Health and Human Services' Office for Civil Rights against a subcontractor for the City's wellness program vendor last week. According to the complaint, the breach occurred when an employee of the subcontractor copied over 9,000 records to a flash drive without encrypting the data and left the flash drive (along with a laptop) in her car. The car was subsequently stolen. The flash drive contained names, addresses, dates of birth, Social Security numbers, and the gender of City employees and their spouses/domestic partners. City officials indicated in the complaint that the City and the wellness vendor itself had encrypted or password protected the data prior to allowing the subcontractor access.

Although the subcontractor reported the breach to the Office for Civil Rights—it is posted on the "Wall of Shame"—the City argued in the complaint that the subcontractor should have reported the breach to the police (if not to the wellness vendor and the City) when the police investigated the car theft, twenty-four days before the breach was reported. The City referred to this as an "extreme delay."

According to the Milwaukee Journal Sentinel, one couple has already filed suit against the subcontractor and the wellness vendor. The couple's attorney plans to seek class-action status for the case. Click here for the Milwaukee Journal Sentinel article on the matter.

Wellness Programs and Other Types of Health Plans Subject to HIPAA

The complaint illustrates one result of the HITECH Act and related Omnibus HIPAA Rule amendments that went into effect in September: increased scrutiny of vendors and subcontractors that administer wellness programs and other programs that are not traditional major-medical health plans but nevertheless qualify as health plans that are subject to the HIPAA Privacy, Security, and Breach Notification Rules. While wellness programs are not always subject to HIPAA as health plans and covered entities, in most cases they are. These wellness programs generally must engage vendors in business associate agreements

that require the vendors—and their subcontractors—to comply with HIPAA requirements. Many such vendors (including subcontractors) lack the sophistication to meet all applicable HIPAA requirements.

In addition to wellness programs, similar issues often arise with administrators of Flexible Spending Arrangements (FSAs) and Health Reimbursement Arrangements (HRAs). Like most wellness programs, these arrangements are group health plans subject to HIPAA as covered entities. On the other hand, vendors generally are **not** subject to HIPAA solely as a result of administering Health Savings Accounts (HSAs). But, while the HIPAA Privacy Rule generally prohibits health plans from disclosing protected health information to HSA vendors, some vendors that administer FSAs, HRAs, and HSAs apply the same privacy policies to all three types of programs—creating risks for health plans that work with them.

Understanding HIPAA Implications and Vendor Risk

Health plans that work with wellness, FSA, HRA, HSA, and other vendors of ancillary products should ensure that they understand how the HIPAA Rules apply to those relationships as well as how the Rules apply to their customers—the employers and others that sponsor the wellness programs, FSAs, HRAs, or HSAs. When contracting with vendors for these products, it is also prudent to obtain appropriate assurances about the vendors' sophistication with respect to HIPAA compliance.

* * * * * * * * * * *

For more information, please contact Tom Bixby at (608) 661-4310 or
TBixby@tbixbylaw.com