wiley

NEWSLETTER

Health Care, Employers, Confusion, and Controversy

March 2014

The recent controversy about AOL CEO Tim Armstrong's comments on employee health care expenses reflects ongoing confusion about the rules for employers and the protections for employees' health care information. As employers become more involved in the overall management of employee wellness and overall health care expenditures, this confusion is likely to remain. *Employers need to very carefully consider their approach to employee health care information and how they will act effectively and intelligently in this controversial and risky area.*

The AOL Incident

AOL's CEO was quoted recently as saying:

Two things that happened in 2012. We had two AOL-ers that had distressed babies that were born that we paid a million dollars each to make sure those babies were OK in general. And those are the things that add up into our benefits cost. So when we had the final decision about what benefits to cut because of the increased healthcare costs, we made the decision, and I made the decision, to basically change the 401(k) plan.

See Ohlheiser, "Did Tim Armstrong's 'Distressed Babies' Comment Violate HIPAA Privacy Laws?," available here.

The media quickly went into overdrive. The big question was whether the comments reflected a violation of the HIPAA rules. For better or worse, there was simply no way to tell from these comments on their own whether HIPAA was violated. At the same time, much of the uproar was about a "violation" of the employees' rights, independent of the actual regulations. Was this an appropriate thing for the CEO to know and speak about? Companies across all industry segments should see this situation as a call to review the governing principles and assess their overall approach in this area.

Several key points lead to the bulk of the confusion.

HIPAA and Employers

First, it is important to understand that the original HIPAA statute does not regulate overall medical privacy. As a result of various choices in the original statute, the law and the accompanying regulations protect health care information in certain settings when held by certain kinds of entities. While the regulations provide substantial protections where they apply, there are large areas of health care where the HIPAA rules simply do not apply.

From the start of the HIPAA regime, employers were a key gap. One of the U.S. Department of Health and Human Services' (HHS) primary concerns in structuring the Privacy Rule was its recognition that employers provide much of the health care in this country. The core purpose of this Rule as it pertains to employers is to ensure that health information is not used against employees in connection with their employment. However, in the HIPAA law, Congress gave HHS no authority to regulate employers at all. Instead, Congress allowed for the regulation of "health plans," including the group health plans defined by the law that provide health care benefits to employees. HHS, therefore, regulates these group health plans, and regulates the flow of information between the health plans that simply provide benefits and the employer that sponsors the health plan and presumably can engage in adverse actions such as terminations.

The core problem is that the line between the "group health plan" and the employer/plan sponsor is a legal fiction. HHS has established a regulatory framework, covering virtually every employer that provides any kind of health benefits to its employees, which is based on the idea that there is a distinction between this "group health plan" and the "plan sponsor" of that health plan. And, throughout the employer community, there simply is no such distinction. The group health plan is a piece of paper, a formal contract required by the ERISA statute, but typically nothing more. It has no employees, and no one with a business card that says, "I work for the group health plan." So, HHS has created a complicated set of regulatory provisions based on a legal fiction. Therefore, there has always been real confusion about even these core rules.

In addition, at the time of the original HIPAA rules, many employers, typically those that were insured plans (rather than self-funded), in fact received little information about individual employee behavior or any detail about employee claims. Now, more plans are self-insured, with a more active employer role in managing plan costs, and even insured plans typically engage in more active oversight of their costs.

In addition, because of the gaps in HIPAA scope, there have always been large areas where employers obtained health care information about employees outside the reach of the HIPAA rules. Disability claims, workers compensation claims, Family and Medical Leave Act data, information obtained as a result of applications, and general information obtained through the course of being an employer all are outside the scope of HIPAA.

The growth of wellness programs has complicated this situation even more. Now, while there are significant restrictions on how these wellness programs can work, the core question of whether wellness programs are in or out of HIPAA remains unclear and confusing. If for no other reason, because wellness programs typically

are offered to employees whether they are covered by the health plan or not, by definition these programs often are not part of the HIPAA structure. These wellness programs also have their own independent set of regulatory complications, which creates additional confusion.

Then, there is the whole sense of employee rights in this area. This is a perception issue, more than one of legal rule. While the question of whether there was a HIPAA violation remains unclear (as there is no clear information indicating that the AOL CEO had any idea who these two people were), clearly, the controversy stemmed in large part from simply bad public relations. The CEO should not have isolated specific employees, even if they were not named (the identity of one of the individuals became public through her own release of information to the media).

And, by publicly using these examples, this situation highlighted the employee concerns and perceptions that employers were acting incorrectly or in ways adverse to employee rights. But was this fair? If the employer is footing the bill, should the employer be able to know general information about overall costs, specific examples, etc. There clearly are limits, from HIPAA and otherwise, about what can be done with this information. If these individuals had been fired because of these expenses, it clearly would have been a violation of various laws. But is simply knowing this information itself any kind of violation? What if this information is used for appropriate management of the health plan only? Would the controversy have been the same if the CEO used the exact same data to seek out a new health care program administrator or alter the overall structure of the benefits plan?

Responding to the Challenges

So, with both the complicated regulatory structure and the overall nervousness among employees about employer behavior, what is an employer to do?

First, employers must analyze what kinds of health care benefits are provided to employees. This analysis must include not only major medical plans, but also vision, dental, group long term care plans, and even "Section 125" plans allowing employees to select certain health care benefits (or other kinds of employee benefits). Now, wellness programs should be evaluated as well.

In general, the Rule creates more obligations for employers that "self-fund" or "self-insure" their employee health care benefits. This is because HHS has assumed (for the most part correctly) that employers that "self-insure" have in their possession health care information about their employees.

Second, try to make some sense of this plan sponsor/group health plan distinction. Most group health plans established by employers do distinguish between the plan sponsor and the group health plan, although this distinction may exist only in legal documents required by the ERISA statute. While the HHS rule does not help much on this point, the "group health plan" should presumably engage in the "day-to-day" operations of the health plan. If your company is fully insured, there may be little to do here, since the health insurer does most of the work. In fact, if your group health plan is fully insured and does not receive protected health information at all, then you can get out of many of the compliance requirements of the Privacy Rule.

The plan sponsor, by contrast, may have "big picture" responsibilities for operation of the plan. The plan sponsor, conceptually, is more like the employer in its traditional employment role. That means that enrollment is one of the functions of the plan sponsor (who also "enrolls" employees in a wide variety of non-health care benefits, such as life insurance or a 401(k)). The plan sponsor also might evaluate overall funding of the health plan, decide to change the benefits structure or alter the benefits package for the plan, or decide to change insurers. HHS recognizes that these functions are "plan sponsor" functions, but believes that many of them can be done without receiving protected health information.

Third, analyze all of the "touchpoints" that your company has with employee health information, whether in or out of HIPAA. You need to consider whether you can do what you need to do without unintentionally creating compliance obligations. For example, many employers will assist employees with questions about their health care coverage, including specific claims information. Presumably, if your company helps employees with these issues and wants to continue doing so, you should make sure that someone who has a "group health plan" can perform these functions. Even for a group health plan, you may need to have your employee sign an "authorization" form, which will allow the health insurer or third party administrator to discuss an employee's claims information with you.

Fourth, focus on the contractual arrangements related to your health care benefit plans. Who is your insurer? Are there multiple companies involved? Do you rely on an insurer to handle day-to-day operations of the plan? Or do you use a traditional third-party administrator? Do you work with an insurance broker of some kind? Or some other kind of consultant that helps you get knowledge about your employee benefit plans and costs? Are you reinsured? Do you have stop-loss coverage for your health plan? Do you work with any employer groups to collectively manage costs? For each of these steps, you need to analyze whether individually identifiable health information is used, and if so, both whether it really is needed and how (if needed) you can continue to obtain and disclose it in compliance with the Privacy Rule.

Fifth, for any situation where your company needs to receive health care information about employees, keep in mind the plan sponsor/group health plan distinction. Which side do you want the information to be on? In general, it will be "better" for the employer to have this information reside on the "group health plan" side, since it is only the "plan sponsor" side that could fire an employee. If there is some particular reason that the "plan sponsor" needs to have this information, analyze the effects of receiving this information (*e.g.*, will a single event mean that you need to comply with all of these rules both as a group health plan and a plan sponsor), and how can you protect the information in the possession of the plan sponsor so that it does not become a problem later on.

Sixth, evaluate alternatives to current health care programs. For example, as the health insurance exchanges expand, will we see employers moving employee health care coverage into these exchanges—and therefore take the employers out of the middle? This clearly will reduce the privacy risks for both employers and employees, as employers will no longer have a basis to receive information or to manage the overall costs associated with employee care. Will this be a smart solution overall?

Conclusions and Key Principles

In the decade since these rules first went into effect, HHS has provided virtually no assistance to help employers, their health plans, and their business associates deal with HIPAA's complexities. At the same time, there has been essentially no enforcement against the group health plans, and generally little controversy in specific situations.

Here are suggestions on some core operating principles for employers generally.

Less Is Better

From a privacy perspective, less information about employee health claims is better. If you can get by with no health information about individual employees, privacy compliance obligations decrease dramatically. If you can't, restrict the information you receive as much as possible.

Whatever Information You Get, Protect It Well

Keep in mind that compliance with these rules is not your only concern. "You violated my privacy" is going to be an increasingly loud refrain in employee litigation across the country, and there is a virtual certainty that most employers will not have "dotted the I's and crossed the T's" to ensure that all of HIPAA's legal requirements have been met. Security breaches also are an increasingly significant concern. If there is a security breach involving employee information, there may be obligations under the HIPAA rules or a wide variety of state laws. These risks are substantial—and are much smaller if you have little or no sensitive personal information.

Understand How You Operate

It is critical for an employer to re-evaluate how their health plan is operated. What information do you receive today? What do you do with it? Do you need it? Who is working for you? How do you relate to your insurer? Understanding the full scope of these activities is essential to making a meaningful effort at complying with these rules, and protecting your company and your health plan.

Recognize the Ambiguities

These rules, in many situations, simply will not make sense or will not fit well with reality. There is a tendency with all involved in HIPAA compliance to simply throw up their hands and walk away. You will want to do this many times. However, keep in mind the primary goal of these rules (to prevent misuse of employee health information), and take the approach that best protects both this information and your company.

Get Help

There are lots of ways to obtain assistance on these issues. Your insurer or third party administrator may be a source of information. Local groups are emerging around the country. Trade associations may be of help. And there is a growing network of attorneys and consultants that can provide advice.

Keep the Final Goal in Mind

Your goal should be to understand these rules as best you can, and to structure your own benefit plans so that you can achieve as much compliance as is realistically feasible, and then to protect your employees' health information wherever possible. Be cautious. You will find that much of the information you receive today is unnecessary or not used. Where you do need to receive information, think about whether there is a way to get what you need without the information being in your company's possession—and particularly not in its employment files.

Be Smart About Public Perceptions

In addition, beyond pure regulatory concerns, the Armstrong story indicates that the most pressing risks may be related to public or employee perceptions. Always think about what you say to and about your employees, and the contexts in which you make statements. Be smart about the information you obtain and about how you use it. Because these rules are so complicated, and because individual concerns about privacy may exceed the reach of the privacy rules, it is critical for employers to act carefully about employee health information. Understanding and acting upon the legal rules is critical, but operating an effective overall program requires much more than simply applying these legal principles.