Making Sense of Employee Health Record Privacy Regulations

By Kirk J. Nahra, JD

Personal healthcare information is inherently sensitive, and individuals are justified in worrying that the breach of such information could result in an impact on their career, personal embarrassment, insurance risks, and a variety of other adverse consequences. Identity thieves, as a result, find healthcare information to be incredibly valuable.

As employers become more involved in the overall management of employee wellness and healthcare expenditures, there is a strong interest in effective management and utilization of this employee data for a growing range of employer interests. Employers and other entities are becoming more involved in Big Data initiatives, offering new opportunities to gather information that will promote more effective and efficient workplaces. However, employers need to consider carefully their approach to employee healthcare information and act intelligently.

For employers, this concern about healthcare information comes with enormous legal, compliance, and related risks and a range of challenges. This article will outline some of the key issues for employers related to employee healthcare information, and will outline some of the key steps to consider in developing an appropriate compliance and regulatory approach for this information.

The Start of the Problem: HIPAA and Employers

Much of the challenge for employers when dealing with employee healthcare information stems from the HIPAA Privacy Rule. When this rule was being written, one of the government's primary concerns in structuring the rule was its recognition that employers provide much of the health insurance in this country. With this background, the goal of the US Department of Health and Human Services (HHS) with employers is quite clear—to ensure, as much as possible, that personal health information is not used by employers for employment-related decisions or used against an employee in connection with their employment.

However, because of the tortured history of the HIPAA statute, which was driven by health insurance portability and "standard transactions" rather than privacy, HHS had no authority to regulate employers directly. If it had been given such authority, the law could have included a provision that said "no employee health information can be used for employment-related purposes." However, this is not the case.

While HHS could not regulate employers directly, HHS did have authority to regulate group health plans, which are the employee welfare benefit plans that provide actual healthcare benefits to employees and define the scope of these benefits. These group health plans are "covered entities" under the HIPAA Privacy Rule, meaning that for the most part they must comply with the HIPAA Privacy Rule to the same extent that a typical health insurer or large hospital must.

Under the HIPAA Privacy Rule as written, employers must place stringent conditions on the flow of employee health information from the group health plan, which is the formal entity providing healthcare benefits to employees, and the employer itself as the health plan's sponsor.

And therein lies the problem. HHS 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 (the federal law governing employee benefits and pension plans), but typically nothing more. So, HHS has created a complicated set of regulatory provisions based on this fiction that there is today an actual or conceptual separation between a plan sponsor and a group health plan.

In addition, because of the gaps in HIPAA's scope, there have always been large areas where employers obtained healthcare information about employees outside the reach of the HIPAA rules. For example, disability claims, workers' compensation claims, Family and Medical Leave Act data, information obtained as a result of employment 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 operate, the core question of whether wellness programs are in or out of HIPAA's purview remains unclear and confusing. 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.

Employers also are using Big Data concepts to gather more information about their employees from a variety of new sources, both regulated and unregulated. So, for many companies, the goal of gathering data and trying to analyze it often runs ahead of responsible and compliant behavior related to the protection of this data.

Responding to the Challenges

So, what is an employer to do? The following are some best practices to ensure proper handling of employee records.

Analyze

Employers must analyze what kinds of healthcare information they have about employees and where it comes from. They should evaluate who manages and operates the health plan and the ways health information is gathered. How is the health plan managed and operated? What other types of health information is gathered from employees? These are questions employers should ask themselves. Assess the data that's being collected and how it's applied to healthcare activities (i.e., behavioral data used to predict employee absences). Examine other collected data and determine whether it could be applied to healthcare activities.

Distinguish

Try to make some sense of this plan sponsor/group health plan distinction. Most group health plans established by employers do have a legal distinction 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 an employer is fully insured, there may be little to do here, since the health insurer does most of the work.

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. The plan sponsor/employer also will be the entity gathering "the rest" of the healthcare information about employees, from all sources other than HIPAA regulated activities (such as medical leave requests, health information on job applications, and other "employer" activities). The plan sponsor 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. These "management" functions may seem appropriate for the plan sponsor.

Examine Touchpoints

Analyze all of the "touchpoints" that an employer has with its employee health information, both within and outside of HIPAA's scope, so as to avoid unintentionally creating compliance obligations. For example, many employers will assist employees with questions about their healthcare coverage, including specific claims information. Presumably, if a company helps employees with these issues and wants to continue doing so, they should make sure that someone who has a group health plan label (and is acting appropriately within the HIPAA environment) can perform these functions. Even for a group health plan, the employees may need to sign an authorization form that allows the health insurer or third party administrator to discuss an employee's claims information with the employer. Review the process of healthcare information flow and evaluate whether there are other places where the company touches healthcare information about employees.

This issue has taken on added importance in a Big Data environment. There are more sources of information than ever before. Virtually all companies would benefit from having a chief privacy official (or someone similar) who can strategize and provide guidance over the full range of data collection issues related to employees.

Risk Management is Vital

On a broader level, for any healthcare information collected about employees, whether regulated or not, the following offers some suggestions on core operating principles for employers.

Less is Better

From a privacy perspective, less information about employees and their health claims is better. For employers that can get by with no health information about individual employees (particularly within the HIPAA regulated side), privacy compliance obligations can decrease dramatically. Employers that can't operate in this fashion should restrict the information they receive as much as possible.

Protect What You've Got

Keep in mind that compliance with these rules is not the 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 Is and crossed the Ts" 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 there is little or no sensitive personal information to worry about.

Understand How You Operate

It is critical for an employer to re-evaluate how their health plan is operated and how any other healthcare information is controlled and used. Employers need to ask themselves: "What information did I receive today? What did I do with it? Do I need it? Who is working for me?" Understanding the full scope of these activities is essential to making a meaningful effort at complying with these rules, and protecting employers and their health plans.

Be Clear to Employees

While HIPAA provides specific rights, most unregulated information is subject to more ambiguous legal principles. While there are many exceptions, employers often can do what they wish in connection with employee monitoring and employee data, as long as they make it clear to employees what they are doing.

Be Smart

At the same time, with this flexibility comes a responsibility to act appropriately, whether for ethical reasons, protection of employees, or concern about potential litigation or enforcement. Always ask why data is being collected, what's being done with it, and whether it all makes sense.

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. This is not unusual. However, it's important to remember the primary goal of these rules is to prevent misuse of employee health information, and take the approach that best protects both this information and employees.

Keep the Final Goal in Mind

Understanding these rules can help employers achieve as much compliance as is realistically feasible. The most important thing is to protect employee health information wherever possible. Much of the data collected by employers is not necessary and goes unused. If a company does indeed need to receive health information, leaders should consider ways to get it and keep it in their possession. Ideally, it should not be kept in employment files. A lot of companies have these challenges, and their circumstances can help educate others.

Thoughtful Decision Making Goes a Long Way

The matter of employee health information is a quickly moving target, given ever multiplying new sources of data and the lack of clear rules around them. But with some forethought and a proactive approach, thoughtful decisions can be made.

Kirk J. Nahra (knahra@wileyrein.com) is a partner with Wiley Rein LLP, based in Washington, DC, where he represents companies in a broad range of industries in connection with privacy and data security laws and regulations across the United States and globally.

Article citation:
Nahra, Kirk J. "Making Sense of Employee Health Record Privacy Regulations" *Journal of AHIMA* 88, no.8 (August 2017): 34-37.