Wiley Rein & Fielding LLP

MAKING SENSE OF HIPAA PRIVACY FOR EMPLOYERS

Kirk J. Nahra[1]
Wiley Rein & Fielding, LLP

In today's health care marketplace, any employer that provides health care benefits to its employees faces new challenges in connection with these benefits, ranging from rising costs to increased risks and benefits of medical technology and the liability risks stemming from the "patients' bill of rights." With all of these challenges, one new dilemma has been overlooked by many in the employer community. This dilemma stems from the privacy provisions of the Health Insurance Portability and Accountability Act ("HIPAA"). The privacy rule, promulgated by the Department of Health and Human Services, does not regulate employers in their role as plan sponsors; it does, however, regulate the group health plans sponsored by these plan sponsors. The privacy rule, therefore, will have some effects on most employers that provide health care benefits to employees, and substantial obligations on many employers and their health plans. The complete effects of these rules will depend in large part on how employers -- wearing both their plan sponsor and group health hats -- address the complex issues and choices presented by this rule.

This article attempts to frame this dilemma for employers and their group health plans, by explaining the basic principles of the HIPAA rule and outlining the challenges faced by employers. The goal is not to provide answers to all of these challenges; instead, the aim is to define the problem, so that employers can address these issues promptly and efficiently -- and with an effective understanding of how best to respond to these challenges in the way that is most beneficial to the employer's overall health care benefits strategy.

The effect of these privacy rules on employers is the single most complicated and confusing element of the entire HIPAA Privacy Rule, which is an extraordinarily complicated rule in its entirety. Because of the breadth and overall complexity of this Privacy Rule, rating first in the "most confusing" category is quite an accomplishment.

---

[1] Kirk J. Nahra is a Partner with the Washington, D.C. law firm of Wiley Rein & Fielding LLP. He is the editor of Privacy Officers Adviser, a monthly privacy newsletter of the International Association of Privacy Professionals. He represents a wide range of insurers, health plans and others on issues related to the privacy and security of information. He can be reached at 202.719.7335 or Knahra@wrf.com.

Accordingly, recognizing that the rule is ambiguous and broad reaching, and that the employer community has not had the resources or knowledge to respond to the full range of compliance challenges presented, this article attempts to make sense of this confusion. The goal is to identify key questions about the HIPAA Privacy Rule for employers, and provide some guidance on how to reconcile the requirements of this Privacy Rule with the day-to-day provision of health plan benefits to your employees. Unfortunately, however, there is little certainty as to how best employers can reconcile the regulatory requirements with the reality of offering a health plan to employees.

The Scope Of The HIPAA Privacy Rule

The HIPAA privacy rule is the culmination of several years of efforts to achieve "administrative simplification" in the health care system. The HIPAA administrative simplification provisions cover the standardization of electronic health care transactions, security of confidential information and the privacy of individually identifiable health information. Because the "standard transaction" rule mandates a movement to electronic claim processing for health care claims, concerns about the privacy of personal health information increased substantially. Accordingly, the HIPAA statute mandated the creation of a federal privacy standard for health information

When Congress failed to pass privacy legislation, the task fell to HHS to develop federal regulations protecting health care privacy. As HHS Secretary Thompson stated in announcing the new privacy rule, "We have laws in this country to protect the personal information contained in bank, credit card and other financial records. Our citizens must not wait any longer for protection of the most personal of all information -- their health records."

Further, according to Thompson, this rule "makes sure that private health information doesn't fall victim to the progress of the information and technology age, where an array of data is readily available in computer systems and too often just a keystroke away from being accessed. We are giving patients peace of mind in knowing that their medical records are indeed confidential and their privacy is not vulnerable to intrusion."

To Whom Does The Rule Apply?

HIPAA limits the direct applicability of the privacy rule to three kinds of entities: (1) health plans, (2) health care clearinghouses and (3) health care providers who transmit certain health information in electronic form. It is the scope of these "covered entities" that begins the dilemma for employers.

A health plan is defined as an "individual or group plan that provides, or pays the costs of, medical care." The HIPAA statute includes a number of examples, including "group health plans," "health insurance issuers," managed care plans, essentially all government health plans and Medicare Supplemental plans. HHS makes clear in the final rule that its jurisdiction did not extend to a wide range of insurance entities that use and disclose health information, and

therefore that the privacy rule does not apply to workers' compensation, automobile, disability or life insurance, even when such arrangements provide coverage for health care services.

Core Facts for Employers

In order to begin to make sense of this confusion, it is critical to understand a few key issues about this Privacy Rule.

First, one of HHS' primary concerns in structuring the rule was its recognition that employers provide much of the health care in this country. With this background, HHS's goal 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. This overriding goal dominates HHS' approach on this issue.

Second, HHS had no authority to regulate employers directly. If so, perhaps a single rule that said "no employee health information can be used for employment-related purposes" would have been sufficient.

Third, HHS did have authority to regulate "group health plans," which are the employee welfare benefit plans that provide actual health care benefits to employees and define the scope of these benefits. These group health plans are "covered entities" under the Privacy Rule, meaning that, for the most part, they must comply with the Privacy Rule to the same extent that a health insurer or large hospital must.

Fourth, because of its inability to regulate employers directly, the core approach of this Rule for employers is to place stringent conditions on the flow of employee health information *from* the group health plan or the health insurer *to* the plan sponsor.

And therein lies the problem. 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 this fiction that there is today an actual or conceptual separation between a plan sponsor and a group health plan.

Fifth, HHS has proposed a compliance regime that mandates full compliance obligations if any employee health information flows to a plan sponsor or group health plan (with minor exceptions), even where an insurer handles virtually all of the work of operating a plan. This "all or nothing" approach forces employers and their health plans to scrutinize every involvement they have with any aspect of the employer health plan.

On top of this regulatory confusion, employers also need to recognize that there has been a fundamental change in the past few years as to how personal information is protected across the country. Through a wide variety of statutes and regulations (affecting health care, financial services, the Internet, employment and otherwise), privacy rights have become a significantly more protected (and publicized) issue. The widespread (and often misleading) publicity surrounding certain aspects of the HIPAA Privacy Rule has magnified interest in these issues. So, employers must not only struggle to understand and apply the HIPAA Privacy Rule, but must recognize that employees (and the lawyers that might represent them) now are using privacy rights as the basis for allegations and litigation against employers. So, notwithstanding the confusion generated by the HIPAA Privacy Rule, employers may wish to reduce the amount of health information in their possession, regardless of compliance with any particular privacy rule.

Responding To The Challenges

So, what is an employer to do?

Analyze

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 or “flexible spending accounts” allowing employees to select certain health care benefits (or other kinds of employee benefits).

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 more possession more health care information about their employees (keep in mind the major goal of this part of the Rule--to prevent employee health information from being used by employers against employees).

Distinguish

Second, 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 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. These "management" functions may seem appropriate for the plan sponsor. HHS recognizes that these functions are "plan sponsor" functions, but believes that many of them can be done without receiving protected health information.

Therefore, for plan sponsors, HHS has created some exceptions to the Privacy Rule. A plan sponsor, in performing its functions, can receive "summary health information" (which is essentially a subset of PHI that summarizes claims history, expense or experience and has been stripped of certain personal identifiers), even though a plan sponsor could "figure out" who particular information relates to (*e.g.*, a claim summary reports one large claim, and only one employee in a small company was out on medical leave for an extended period of time). (As a hint, don't try to figure out whom summary health information is about - it can only hurt you as an employer, if something adverse happens to that employee). Summary health information may be released to a plan sponsor without privacy rule compliance obligations if the plan sponsor agrees to limit its use of the information to (1) obtaining premium bids for providing health insurance coverage to the group health plan; or (2) modifying, amending or terminating the group health plan.

Also, plan sponsors can receive protected health information related to enrollment in the health plan - for example to learn from a health insurer who has enrolled in the plan, or disenrolled, since "managing" overall enrollment is an appropriate function for an employer. If the only PHI a plan sponsor receives falls into these categories, then a plan sponsor does not need to engage in significant compliance activities for the Privacy Rule.

From HHS' perspective, these are "appropriate" functions that do not involve "sensitive" protected health information, or "high risk" information that likely could be used against an employee. If employers -- again wearing their "plan sponsor" hat -- determine that they can effectively manage their benefits program *without* receiving protected health information, then the employer as plan sponsor can avoid many of the obligations imposed by the HIPAA privacy rule. If a plan sponsor needs more information than that, however, for whatever reason, then the plan sponsor has to begin significant compliance activity. A plan sponsor that needs more than these "exception" categories should consult counsel on how to comply with these onerous regulatory requirements.

Touchpoints

Third, analyze all of the "touchpoints" that your company has with employee health information--so that you can make sure that you are doing what you need or want to be doing, without unintentionally creating compliance obligations. For example, many employers will assist employees with questions about their health care coverage, including specific claims information. Is this something that your company does? Who does that in your company? 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" hat 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. Review the process of health care information flow

in your company, to evaluate whether there are other places where your company "touches" health care information about your employees.

Contracts

Fourth, focus on your 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. You also will need to revisit any contracts that you have with these third parties - called "business associates" under the Privacy Rule. You also will want to evaluate how closely you monitor the activities of your insurer or administrator.

Compartmentalize

Fifth, for any situation where your company needs to receive health care information about employees, keep in mind this 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.

Guidance on Making the Privacy Rule Work

Despite my efforts and the efforts of many others to explain this rule to employers, the HIPAA Privacy Rule simply is not a good fit for how health care benefits are provided by employers to their employees. Whether through a focus on other issues or a lack of understanding on how the private insurance markets operate, HHS has provided virtually no assistance to help employers, their health plans, and their business associates deal with these complexities. It is clear that many group health plans are not currently in compliance (for those “large” health plans that had an April 14, 2003 compliance date), and that many “small” health plans will not meet an April 14, 2004 compliance date, both because they may not know about the rules and because of the difficulty of figuring out what to do. And these difficulties are coming at a time where the health care system is under increasing challenge, though rising costs and other challenges, and the focus on privacy rights across the country has made the risks of misuse of employee health information even higher.

No article, particularly a short one, can address all of these issues. Many of the answers will depend on the specifics of what kinds of benefits are provided to employees, how these benefits are funded, how the employer manages the plan, what role an insurer or third party administrator plays in the operation of the plan and the assistance that is forthcoming from this insurer or third party administrator or others. With that said, there are a few concrete hints for employers.

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.

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 trying to make 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, where the rule does not make sense, 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 avenues for assistance on these issues. HHS has promised more, but it is not clear if this will be forthcoming (or, frankly, helpful). 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. You are not alone on these issues.

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. Everywhere 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.

Questions And What Does The Future Hold?

These questions are only the start in the analysis for employer plan sponsors and their group health plans. Will this rule cause the employer make fundamental changes to the health benefits structure for its employees? How will the employer comply with the substantial requirements of the HIPAA privacy statute? If the group health plan uses an insurer or other third party administrator for administration of the group health plan, is that administrator prepared to effectively implement the HIPAA requirements? If the employer has attempted to control overall health care costs through an insurance program that integrates health insurance with disability and workers compensation programs, how will those programs work under the new HIPAA requirements? Are the plan sponsor and the group health plan prepared to "dot the I's and cross the T's" to ensure that these legally required distinctions are enforced in practice?

A few specific areas for consideration.

- Will this Rule affect how employers provide health care benefits to their employees?

You hear the refrain every year – health care premiums are going up again. A major study released in September, 2003 reports that group health plan premiums went up an average of 13.9% in 2003. Will the added costs incurred by employers to comply with the HIPAA Privacy Rule increase costs to such an extent that the health care benefits change? Will fewer employers self-insure (recognizing that the costs of HIPAA compliance for self-insured plans are higher)? Will some employers stop providing benefits at all? How will these costs intersect with the movement toward "consumer directed health plans?" If the risks of HIPAA compliance expand, along with continuing cost pressures, will some employers say the costs and risks are not worth the benefits?

- Will HIPAA affect the ability of health plans to control costs?

Another concern that has arisen is whether employer efforts to control health care costs will be hampered by the HIPAA Privacy Rule. Many employers have developed "disease management" or wellness programs for their employees. Will these programs be able to continue? Will they be as effective? Will the risks outweigh the benefits?

- Will the Rules get any clearer for employers?

As discussed above, the portions of the HIPAA Privacy Rule that affect employers are enormously confusing – more so than any other part of the Privacy Rule. To date, there has been

virtually no assistance provided to employers by the relevant regulators. There have been continued promises that "help is on the way." Will this help be forthcoming? Will employers be able to handle any changes? Will the information be effectively communicated across the employers in this country – recognizing that most employers do not view themselves as being in the health care business?

- How will the HIPAA Rule be enforced?

Another concern is how the Rule will be enforced. To date, enforcement efforts have been limited –focused on responding to complaints, with no public enforcement proceedings since the April 14, 2003 compliance date. Will there be enforcement efforts directed against employers? If so, what areas will the regulators focus on? And will the true enforcement for employers come from lawsuits?

- What is the Future of the HIPAA Privacy Rule?

Since April, the Privacy Rule has generated two basic kinds of complaints – information flow has been too easy, and information flow has been too hard. Regulators and covered entities have been receiving complaints about failures to meet the privacy rule requirements, often from customers or others who have some other "gripe" with the health care system.

On the other hand, a significant number of complaints have been based on a failure of a hospital or health insurer to provide medical information – complaints that are based in part on criticism that the hospital or health insurer IS following the Privacy Rule. The Privacy Rule makes disclosure of medical information harder – and is designed to do so. In some situations, this makes certain "convenient" activities harder to do. Widespread anecdotes have been reported about difficulties in helping parents, children, grandparents, neighbors and friends with their medical problems. Will a sufficient number of complaints in this area lead to a weakening of the Privacy Rule? Or will individual consumers – the supposed beneficiaries of these rules – "get used to" these inconveniences? There also have been limited reports of how "HIPAA confusion" has affected medical treatment – particularly where medical providers will not communicate with other providers with needed treatment information. These kinds of concerns threaten the viability of this rule if they become widespread – particularly given the substantial costs imposed by the Privacy Rule for compliance.

Conclusion

The Privacy Rule is a confusing, complex and broad-reaching regulatory requirement that will affect every aspect of the health care system for many years to come. Employers face dramatic challenges in adjusting their operations to this rule, even though providing health care benefits typically is a minute portion of a company's operations. It also is clear that little guidance is coming from the government on how to make sense of this rule, and prompt changes to the rule to simplify compliance obligations do not appear to be forthcoming.

For employers, therefore, it is important to be careful, cautious and open-minded. Despite an April 14, 2003, compliance date (or another year for "small" group health plans paying claims of less than $5 million per year), it is clear that compliance efforts will continue for several years to come. There also likely will be operating confusion, as employers, their insurers and third party administrators, their agents and consultants and their employees all struggle with these new requirements. The best advice is to recognize the primary areas where this rule can get an employer in trouble (using health information against an employee), and to be cognizant of all of the aspects of your business where your company may come in contact with health information about employees. For these "high risk" areas, a little common sense, along with a basic understanding of the Privacy Rule, should go a long way.