Entering the World of Privacy…
Gearing Up For HIPAA's Privacy Rules

Employers, Providers, and the Health Insurance Industry Take A Deep Breath and Begin to Learn the New Rules…

By: Dorothy M. Cociu, RHU, REBC
President, Advanced Benefit Consulting & Insurance Services, Inc.

So what is all this talk about privacy?

The privacy issue stems from a myriad of recent state and federal actions to protect the privacy of consumers' personal information. Two federal laws, the Financial Services Modernization Act of 1999 (Gramm-Leach-Bliley Act - GLBA) and the HIPAA Medical Records Privacy Final Regulations, released in August, 2002, as well as many state laws, will affect the way we live, work, and receive medical care. Sound complicated or confusing? Let's try to unravel some of the complexities….

Federal Privacy Laws

The GLBA actions relate to financial services; banks, financial institutions, insurance companies, and health insurance agents must comply with a series of privacy requirements and must disclose to their customers in a privacy notice their privacy practices. This is the law that resulted in the vast mailings from banks last year telling us of their privacy practices. Unfortunately, what most consumers don't know is that by throwing those notices into the trash, they literally threw away their rights. Many banks and financial institutions' privacy practices allow them to share your personal financial information, including your bank account balances, loan amounts, and credit ratings, to their affiliates and others *unless you completed and returned the opt-out form contained somewhere in the midst of those many pages you received in the mail, and likely filed in the circular file we call waste cans. Be aware, and the next time you get those privacy notices, be sure to read them!*

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) included several requirements geared toward administrative simplification, basically with the intent of reducing health care costs by requiring electronic processing. Out of administrative simplicity came standards for privacy, security and electronic transaction standards. Electronic Data Interchange (EDI) went into effect on October 16, 2002 for large plans, and is scheduled to go into effect on October 16, 2003 for small plans (and those large plans which filed the appropriate extension with the Department of Health and Human Services (HHS) on or before October 15, 2002). The privacy components are now being rolled out, although the security regulations, as of the date of this article, have not yet been published.

Medical Records Privacy Overview

On August 14, 2002, HIPAA's long-awaited medical records privacy final rules were released. Thankfully, the final rules resulted in a much less cumbersome set of

requirements than originally anticipated, although there seems to be disagreements with intent and actuality within the legal community, the health insurance industry and the regulators.

Medical Records Privacy has an effective date of April 14, 2003 for large plans, and April 14, 2004 for small plans. Unlike many other regulations, these take effect on the actual date – April 14 – not the first day of the plan year following this date.

Medical records privacy includes requirements for transferring data electronically, adopting medical code sets, developing standards for unique identifiers for employers and health care providers and, in some cases, individuals, creating safeguards to protect confidential information, developing standards for transmission of electronic signatures, and protecting individually identifiable information, such as social security numbers, names and addresses.

The privacy rule creates national standards to protect individual's medical records and other personal health information. It gives patients more control over their health information, sets boundaries on the use and release of health records, establishes safeguards that providers and others must achieve to protect the privacy of health information, holds violators accountable with civil and criminal penalties, and strikes a balance when public responsibility supports disclosure of some forms of data.[1]

In general, the HIPAA privacy rule will require providers and plans to notify patients about their privacy rights and how their information can be used, to adopt and implement privacy procedures for its practice, hospital or plan, to train employees so that they understand the privacy procedures, to designate an individual to be responsible for implementation, and to secure patient records containing individually identifiable health information.[2]

So, to assist you as you roll up your sleeves and begin to dig in….Let's learn about HIPAA's answer to "administrative simplicity" and the changes it will bring to the way we deliver and manage health coverage.

Privacy Officer

One of the most important items that plan sponsors must understand early is that they need to make some initial decisions, including the appointment of a "privacy officer." That individual must decide on the proper individuals who will be handling the administration of the plan and potentially have access to restricted data up front. Those individuals will be subject to the privacy rules, and *each individual must be properly trained on privacy rules and practices, and retain proof of such training in their compliance files.*[3] Once this initial decision is made, many, many decisions will need to follow for privacy implementation.

---

[1] OCR HIPAA Privacy, December 3, 2002
[2] OCR HIPAA Privacy, December 3, 2002
[3] 45 CFR Sec. 164.530(a)(1)(i)

Key Terms and Concepts
There are a few key terms and concepts that employers/plan sponsors, plans, agents, and providers must learn to understand, and will be defined below, including protected health information (PHI), covered entities, permitted uses, business associates and TPO (treatment, payment, or health care operations).

Covered Entities
A covered entity is able to access information for certain permitted uses and cannot disclose protected health information (PHI), except under certain exceptions, including business associates and public policy exceptions. Covered entities include health plans, health care clearinghouses, and healthcare providers. Interestingly, employers are not, by definition, covered entities, which leads to greater confusion. Unlike ERISA, privacy requirements stem from the plan, as a covered entity, not the employer.

Protected Health Information
The administrative simplification requirements cover individually identifiable health information, which relates to an individual's past, present or future physical or mental health condition, to the provision of health care to that person, or to the past, present or future payment of that person's health care. When this information is used or disclosed by a covered entity, a plan sponsor, or a business associate, it becomes "protected health information," or PHI.

PHI is individually identifiable health information that is maintained or transmitted by a covered entity. Once it is de-identified, such information can be exchanged. Information can be "de-identified" by removing all the individual identifiers, such as a social security number, a name, or an address.

Permitted Uses for PHI
PHI can be used or transmitted for certain permitted uses, including treatment, payment, and health care operations (TPO). Health care operations include auditing, credentialing, and obtaining reinsurance. All other uses require individual authorizations.

Clarification of the Plan Sponsor Role
As I stated above, covered entities do not include employers. The employer in its entirety is not subject to the HIPAA privacy rules. Privacy is focused on the covered entity, i.e. the plan, and not the employer, unlike ERISA. However, the plan sponsor personnel dealing with PHI are subject to HIPAA, and plan sponsors must create "firewalls" between covered and non-covered functions. Information cannot be used for employment purposes or for purposes of administering any other plan, such as disability or workers' compensation. Health plans cannot share PHI with the plan sponsor unless the sponsor certifies that the plan has been amended limiting use and disclosure of PHI and that the proper safeguards are in place.

The burden of compliance on group health plans and their plan sponsors will vary depending on the sponsor's role in the plan's day-to-day administration of the plan and whether the plan is fully insured or self-insured. A plan and its sponsor may avoid many,

but not all, of the privacy requirements if the plan is fully insured and the plan sponsor has no access to PHI other than summary health information and enrollment information. Self-insured plans will be required to comply with virtually *all* of the privacy standards.

The determination of the "hands-on" or "hands-off" approach is required up front with the selection of the privacy officer. Caution here is suggested, as once the proverbial line is crossed, the plan will likely be required to comply with the hands-on duties. In fact, I question whether even small plans will be able to truly adopt the hands off approach. In a recent interview with Sheldon Emmer, managing shareholder of Emmer & Graeber, an employee benefits law firm in Los Angeles, I asked if he thought even the smallest of employers, or those with HMO's, would be able to realistically use the hands-off approach successfully. "I'm not even sure *they* [the smallest of employers] will. It's certainly a legitimate business decision, but even if we assume that that's the decision, what are you going to do when John Doe walks into H.R. and says 'Can somebody help me with my claim?' Or when John Doe walks in from a 5-day sick leave and the employer says 'where's your doctor's note'? Is that getting their hands on something? Even with the best of intentions, the employer who says I don't want to have anything to do with this, I want to stay out of it, hands-off, are they going to hire an administrator, not to just administer the plan but to handle day-to-day HR functions, with their employees, which even may be at the water cooler? It's an option, and it sounds good until the actual implementation."

The privacy rules generally prohibit a group health plan from sharing PHI with a plan sponsor, except under certain circumstances, including summary health information, enrollment information, and plan administrator functions, where the plan document is amended and firewalls are in place. Summary information refers to summarizing claims data and histories, expenses, or types of claims by individuals. Being summarized means that you have no actual knowledge of individually identifiable information; i.e., it's been "de-identified."

Modifications to the Privacy Rule

Based on the many comments received during the comment period, several provisions were modified in the August, 2002 final rules. Changes include uses and disclosures for treatment, payment and health care operations (TPO), notices of privacy practices, uses and disclosures for marketing purposes, minimum necessary uses and disclosures, uses and disclosures for research purposes, special transition provisions, including business associates agreements, and a list of technical corrections.

Were these changes as good as everyone thinks? I personally believe they were a huge step in the right direction, especially for health agents and employers, but there are genuine concerns. Mr. Emmer had an interesting perspective on the modifications. "We have regs coming out in December of 2000, and everybody is yanking their hair out for a number of reasons. Number one, we don't want to have to do this, number two, wishfully thinking this is going to go away like Section 89, number three, we in the benefit business are now, after all these years, pretty used to IRS and DOL talk. This is coming from HHS. They are not talking the same way. What's a plan? We know what a

plan is for ERISA purposes, but do we know what a plan is for this? The whole concept of 'it's not the employer that has to do anything, but rather the plan…' How many plans have employees to do this? It's really the employer who has to do this, despite what they say. Here we have these December 2000 regs with something like 50,000 comments, and all these comments were absorbed by HHS, to then come out with new proposed regs in March of 2002, which were supposed to be better. In a combination of 'this is still going to go away ala Section 89' and burying their head in the sand in denial, people said 'I'm not sure how much better this is. This is supposed to be administrative simplification and it's not simplifying anything.' Then we get the final regs in August, after a big build-up to it, and everyone was hoping it would disappear, or if not disappear, at least be easier to manage. It's supposed to be better and easier, and I don't know if it's better, and I don't know if it's easier, because it's still so confusing."

Business Associates

Most health care providers and health plans do not carry out all of their health care activities and functions themselves; they often use a variety of persons or businesses. A business associate is a person or entity that performs certain functions or activities that involve the use or disclosure of PHI on behalf of, or providing services to, a covered entity. The privacy rule allows covered providers and health plans to disclose PHI to these "business associates" if they obtain satisfactory assurances that the business associates (BA's) will use the information only for the purposes for which they were engaged by the covered entity, that they will safeguard the information from misuse, and that they will help the covered entity comply with some of their duties under the privacy rule. Covered entities are allowed to disclose PHI to an entity in its role as a business associate only for the purposes of helping the covered entity carry out its health care functions. The business associate is not allowed to use the information for its own independent use or purposes. Examples of business associates include a third party administrator that assists with claim processing, a CPA firm providing accounting services to a plan or health care provider with access to PHI, an attorney providing legal services to a health plan that involves PHI, an independent medical transcriptionist that provides transcription services to a physician, a pharmacy benefits manager that manages a health plan's pharmacy network, or a health insurance agent that is asked to help resolve a claim dispute.[4]

Who Should Be Concerned?

If your plan is self-insured, the plan sponsor needs to be primarily concerned with privacy laws. In an insured health plan, the insurer or HMO should be primarily concerned, although the plan has some requirements. Providers who transmit oral or written health information have privacy considerations. Business associates providing covered services must have their written agreements in place by the compliance date (or possibly sooner, due to transitional rules), and health care clearinghouses have privacy requirements. In general, it affects the entire industry and all employers with a group health plan.

[4] OCR HIPAA Privacy, December 3, 2002

Effective Dates
Providers, clearinghouses, and health plans with annual receipts of more than $5 million need to comply with the privacy rules by April 14, 2003. Health plans with annual receipts of $5 million or less have a one-year delay, and must comply by April 14, 2004. All entities (including large health plans) who must comply with the rules governing Electronic Data Interchange (EDI) were to comply by October 16, 2002, unless they filed a one-year extension with DHHS by October 15, 2002. Health plans with annual receipts of $5 million or less must comply with EDI rules by October 16, 2003. The date of release of the security regulations is unknown at this time.

Will employers be ready? The largest of employers have until April 14 of this year to comply. Is that realistic? "I think it's realistic from the government's standpoint," Mr. Emmer said, "because it says, 'We didn't tell you to wait this long. We've been telling you this since 1996 when HIPAA passed… This is what we've been telling you for years. Don't wait until the end.'"

I think that much of the procrastination of employers stems from their ignorance of the requirements, as well as plain old discomfort. "When you go back to the early days of ERISA, people were just as uncomfortable," commented Mr. Emmer. "Maybe over time, with ERISA we have a better comfort level, and maybe that's what will happen here. The problem that I have with all this is people don't know what they don't know. They don't know how to handle these situations. The people who have written all this, I don't think have written this with much practical experience or much concrete application in mind. It doesn't sound like the people who wrote these regs have a clue about day-day personnel, HR, [and] benefits matters in an employer."

Definition of Small Plans
45 CFR Section 160.103 defined last fall a small health plan as "a health plan with annual receipts of $5 million or less." In general, this refers to $5 million in claims for self-insured plans in the last plan year, and $5 million in paid premiums for insured plans (including HMOs) in the last plan year. For details on reported receipts rules, see the guidance provided by the Small Business Administration at 13 CFR Section 121.104.

The definition of small plans is key, as *it is the single definition that determines whether a plan has to comply by April 14, 2003 or has a one-year delay to April 14, 2004.*

Multiple employer plans will be even more difficult for people to grasp, as the plan may be greater in receipts than the $5 million mark, yet the small employers who may participate may have been, on their own, a small employer, and not subject to the privacy rules for another year. In this situation, being in a large multiple employer plan may hurt the smaller employer.

Responsibilities
The responsibilities vary by the type, funding and size of the plan, and whether the plan sponsor adopts "hands-on" or "hands-off" practices and policies. In general, however, plans must keep records of compliance activities and submit compliance reports to HHS,

cooperate with HHS in investigations or compliance reviews, permit access by HHS during normal business hours, and amend plan documents and Summary Plan Descriptions (SPD's) for compliance. Although the Security Regulations aren't yet released, in general, plans will need a compliance plan for protected information, including making reasonable accommodations to assure security and confidentiality, and must arrange for appropriate administrative, technical and physical safeguards to protect the privacy of protected information. Some of these requirements include decisions on unauthorized access, company practices, access to electronic data, authorization of users, password protections, software safeguards, and physical security, including the location, procedures, key access, file cabinet security, destruction of old data disks, training, etc.

Total compliance will require a detailed action plan (ours for our clients is nearly three pages in length, with 10 point font, bullet-points only), and plans should begin implementation early, as there are lots of items to accomplish. I am recommending, for example, three to twelve months; less for fully-insured, and much greater timelines for self-insured plans.

Authorization Requirements

For circumstances not involving TPO, you must retain an authorization for use. The authorizations must clearly describe the scope of the information and its anticipated use, must be revocable at will, and must include an expiration date. There are a list of authorization requirements in the regulations, but to date, HHS has not issued a model authorization form. There are many confusions in the authorization area; we are currently awaiting additional clarification from HHS.

Areas of Confusion

There are many areas of confusion, which will hopefully get unraveled in time. How do we address the cross-overs into areas of other federal laws, such as the administration of FMLA or the ADA requirements? "I think that currently a lot of the confusion we are seeing from our clients is, how do we do HIPAA privacy and administer FMLA, for example, at the same time? We know that under that FMLA we're entitled to only grant FMLA leave for serious health conditions of yourself or a close family member," stated Mr. Emmer. "How much information are we entitled under HIPAA privacy to find out? When are we wearing our health plan hat? Are we forced to take the word of our employee, saying trust me it's a serious health condition, but you are not entitled to know what it is because it's private…" Suddenly, the HR representative has access to, or just heard about, PHI. "It's the same thing with ADA. How are we supposed to 'reasonably accommodate' someone if maybe we can't ask them exactly what their condition is…? There is an overlap between HIPAA and other federal laws, but I don't think anybody has really been focusing on it."

Another concern is the authorization confusion. When do you really need an authorization? The regulations do not seem entirely clear, and we may see carriers and others doing blanket authorizations with renewals just to be safe, but will they apply in every situation? "You read the regs and you see all these procedures and circumstances and you try to sort them out, and I'm not clear on some of these things," Mr. Emmer

stated. "When does the exception swallow the rule? We are told you can't use individually identifiable PHI, without authorization, except payment, treatment and plan operations. What is plan operations? Isn't that everything? Couldn't you argue that everything is a plan operation and we never need an authorization? The way things are, I don't think it's clear when we need an authorization and when we don't. We're supposed to need an authorization except for things that are so broad, we have a hard time figuring out a circumstance that it's not arguably excepted."

New guidance has been issued, but will the guidance help us in a lawsuit? According to Sheldon Emmer: "Regulations go through an administrative process and as a result, when a court hears a lawsuit, the court is supposed to give some deference to the regulations of the agency who is in charge of the enforcement and issues the regulations, because they have gone through this administrative process. A court can say the regulations have exceeded the scope of the statute, but if the regulations have not exceeded the scope of the statute, then because of this 'administrative process', courts are supposed to generally follow them. That's only true with regulations. These guidances and guidelines and Q's and A's and FAQ's are not regulations. The courts need not give precedential deference to anything that is not in the final regs….If it's not a reg, a court doesn't have to pay any attention to it."

So how do employers comply? Personally, I think "good faith efforts" will be the key, especially initially. Employers will need to start making decisions, get trained and start the "to do" list, and "Action Plan". But that doesn't mean it will be an easy, simple process. And each situation will be handled independently.

"You'd think that a reasonably educated person should be able to go through this, with the general concept that we're trying to protect people's privacy, and say, okay, this is what we have to do,"stated Emmer. "But because this is so fact driven, with so many exceptions, and so many twists and turns and loopholes, from the view of the legal community and in the employee benefits industry, it's not a whole lot better. In my opinion, they've done a terrible job in instructing the country how to comply with this law.

"People are still hoping it's going away, and now getting the sinking feeling it won't, but trying to scratch and claw their way through it and figure out what they're going to do, and there are more unanswered questions than answered questions. That's why I think there is confusion out there."

The Bottom Line

Unfortunately, it's here to stay, and we have to dig in and deal with it. Whether or not your firm is a covered entity, the bottom line is, any employer with a group health plan will need to learn about privacy, and quickly. And keep in mind, *this is all about "administrative simplicity!"* Before you completely panic, let me share with you something I learned from my Algebra One teacher back in Junior High School. There I was, about to fail a class for the first time in my young life, and I was panicked. My teacher, knowing I was a good student, took me aside after class not a week before my

mid-term and said "Dorothy, you are making this too difficult. You are over-analyzing this thing." (*Imagine that; he had me pegged as an overly-analytical detail-fanatic before I was a teenager*). "Just learn the rules, and play the game." I must have looked confused, knowing in my heart at that young age *that in my world, x would never equal y*, and he reassured me with "This thing is only algebra. It's just a game. Learn what each piece means. *Learn the rules, play the game….*" And I did. He kept me after school for a week, and worked with me until I finally got it. Every time I tried to out-think the game, he said the same thing…"Learn the rules, play the game…" So, I'm sharing this wisdom with all of you. And if Mr. Call in Oxford, Michigan, my junior high school algebra teacher, should ever hear of this, thank you for that wonderful lesson. I'd like to pass on similar wisdom to you…..

Yes, there is a lot to accomplish. But you can. It's not brain surgery. It's a new health plan law. Learn the rules and play the game. Just like we did when COBRA was enacted. Remember that? Most of us panicked, thinking our worlds were about to collide. But they didn't. We learned the rules, and we played the game. Now, you are beginning to learn the rules. *Let's play…..###*

Special thanks to Sheldon Emmer, shareholder in Emmer & Graeber, an employee benefits law firm in Los Angeles, California (310) 475-3792.

About The Author:

Dorothy M. Cociu, RHU, REBC is an employee benefit consultant and employee benefits instructor in Southern California, specializing in mid-size and large group health plans, with an emphasis on self-insurance and HIPAA compliance. Her firm is a provider of HIPAA Privacy Training for Privacy Officers and their Privacy Teams. She is the founder and president of Advanced Benefit Consulting & Insurance Services, Inc., with offices in Orange County and San Bernardino County, in Southern California. She is a national speaker on health care issues, particularly HIPAA,COBRA and other federal topics. Dorothy is the author of The ABC's of HIPAA Compliance; A Simplified Employer Guide to HIPAA Compliance. She can be reached at Advanced Benefit Consulting at (888) 288-0164 in Orange County, or (866) 658-3835 in San Bernardino County, extension 3#, or at dmcociu@advancedbenefitconsulting.com. Her company's website and employer seminar listing, including privacy officer training, can be found at www.advancedbenefitconsulting.com.

Reference Sources:

- *Federal Register, August 14, 2002 (Volume 67, Number 157), Rules and Regulations, Part V, Department of Health and Human Services, Office of the Secretary, 45 CFR Parts 160 and 164; Standards for Privacy of Individually Identifiable Health Information; Final Rule, RIN 0991-AB14*
- *US Department of Health and Human Services, Office of Civil Rights, Medical Privacy, National Standards to Protect the Privacy of Personal Health Information, OCR Guidance Explaining Significant Aspects of the Privacy Rule, December 3, 2002*
- *HHS Fact Sheet, US Department of Health and Human Services, August 9, 2002, Modifications to the Standards for Privacy of Individually Identifiable Health Information – Final Rule*
- *Small Business Guidance on Small Health Plans, 13 CFR Section 121.104*

This article is being published in Health Insurance Underwriter (HIU), March, 2003, as well as a number of other publications, including Human Resources publications, locally and nationally.