Since late December 2000, all of us in the health care industry - providers, insurers, clearinghouses - have had to focus much time and effort on HIPAA compliance. We have repeatedly read and re-read the HIPAA Privacy Rules, attended numerous seminars and teleconferences exploring various nuances of the Rules, worked with our attorneys, performed our gap analysis, developed our policies, procedures and forms and discussed among ourselves the practical application of these sometimes difficult to understand regulations. We have submitted comments to the current and proposed Privacy Rules and avidly read last March’s NPRM, as well as the recently released Privacy Rule final modifications.

So, as we enter the home stretch in HIPAA Privacy compliance, living with the HIPAA Privacy Rules should get easier, right? Unfortunately, that’s not exactly true. There are a few lessons that the health care industry has learned on the road to HIPAA Privacy compliance and a few myths debunked as well.

This article will offer some insight into the issues that the health care industry has been struggling with over the past 18 months, along with a few tips on how the health care subrogation industry can work with their health plan clients in the brave new HIPAA world.

*Nothing endures but change. - Heraclitus.*

As this article was being prepared for publication, HHS released its long-awaited first set of modifications to the Privacy Rules. A new concept, that of “limited data set,” was introduced, with corresponding new rules for its use by covered entities. Significant changes were made to the consent requirement for health care providers, authorization forms, business associate agreements, the rights of parents to minors’ protected health information and the definitions of hybrid entity and marketing activities. Minor changes were made in the areas of minimum necessary, health care operations, disclosures between covered entities, group health plan rules and disclosure accounting.

Because the new modifications will be published in the Federal Register on August 14, 2002 and due to the 60-day period under the Congressional Review Act, covered entities will need to comply with these new modifications by April 14, 2003. For those covered entities, particularly health care providers, that just spent the last 18 months planning how to modify their procedures to comply with the previous iteration of the Privacy Rules, these modifications represent an expensive and frustrating retrenching and reworking of their compliance plans over the next eight months. For health plans, the retooling will not be as extensive, but some modification of current policies, procedures and forms will still be necessary.

While change is inevitable, particularly with respect to laws and regulations, it would have been easier and certainly more cost-effective, particularly for the provider community, to be able to complete one action plan rather than modify plans already partially completed.

*HIPAA is not really “all about standards.”*

I used to preface my presentations about HIPAA Administrative Simplification with the oft-quoted statement that “HIPAA is all about standards.” I would mention that the intent behind the HIPAA Transaction Standards rules was (simplistically speaking, of course) to have all the computers in the health care industry speaking the same ANSI X12 language and that HIPAA Privacy was intended to institute comprehensive federal privacy protections so that all players in the health care industry would guard protected health information the same way.
Over the past 18 months, the health care industry has learned that while HHS’ intent was to set standards, the reality is far different. The HIPAA Transaction Standards Rules allow the eight HIPAA standard transactions to contain optional “situational” elements that can differ from trading partner to trading partner. The HIPAA Privacy Rules contain a preemption provision making applicable state laws that are “contrary” to and “more stringent” than the Privacy Rules VII, so that sometimes the federal rules will apply and sometimes state laws will apply, with not much predictability as to which law will apply in which circumstances. Even the definition of “more stringent” VIII is not uniform. (More on preemption later.)

In Wisconsin, for example, a state statute applicable to insurers requires a health insurer to modify the HIPAA standard authorization, as well as its procedures concerning individuals’ rights to access, amendment and disclosure accounting IX. This statute, however, does not apply to health care providers.

Such lack of consistency can lead to anomalous results. If an insurer offers an authorization incorporating HIPAA and state law provisions to a health care provider, the provider could potentially refuse to accept it, due to the state law provisions included in the form. From the provider’s perspective, those additional state law provisions do not comport with HIPAA. We thus may have providers and health insurers needing to use different types of authorization forms due to this stricter state law.

Rather than applying just one federal legal privacy standard, such as Congress envisioned with ERISA in the area of employee benefits, HIPAA Privacy covers us with a patchwork quilt of federal, state and territorial laws, regulations, case law, constitutions and Attorneys General opinions. HIPAA Privacy preemption is enough to frustrate even an experienced health care lawyer, much less a health insurer or health plan trying to devise a practical, standard approach to privacy while doing business in several states.

**Different organizations have different interpretations of the Privacy Rules.**

Not only do different types of organizations construe HIPAA Privacy provisions differently, but interpretations vary among similar types of organizations. Just as corporate culture varies, so do organizations’ tolerance for acceptable legal risk. Even when the Privacy Rules do set a federal standard, there are almost more questions than answers about the standard and it is difficult to get guidance from the few, albeit dedicated, staffers at OCR. Participation at seminars and in Internet list servs yields much and oftentimes spirited discussion but usually no consensus. Even reasonable lawyers differ on their interpretations.

In attempting to deal with different clients’ expectations, a subrogation company may want to establish internal HIPAA Privacy “best practices,” so as not to incur too much administrative time handling similar clients differently. For example, a subrogation company that is a business associate will need to be aware that they need to assist their health plan clients in providing individuals with access to the protected health information in the subrogation company’s possession. X The subrogation company could decide to either provide access to individuals directly pursuant to the Privacy Rules or simply provide information to the health plan upon their reasonable request.

**Business Associate Agreements are not alike.**

Most subrogation companies that are not members of a health plan's workforce will be “Business Associates” XI of a client health insurer, HMO or self-insured group health plan. By now, most in the health care industry have seen a variety of flavors of business associate contracts and it is clear that every organization wants to say the same things required by the HIPAA Privacy Rules in many different ways.

Early on, our organization was surprised to receive from a document retention and storage facility, a business associate agreement that omitted most of the HIPAA-required provisions. This was puzzling, since it was a
fairly large national organization proposing the agreement. Their reason for doing so? They could not
currently comply with all the business associate provisions, so they only incorporated into the agreement the
HIPAA provisions they could comply with at that point. I've often wondered when or how they thought the
other required business associate provisions would get into the agreement. A much better idea, which we
ultimately suggested, would have been to make the entire business associate amendment effective as of April
14, 2003, the compliance date for most covered entities subject to the Privacy Rules.

The sample business associate language issued by HHS in the newly-released Privacy Rule modifications XII
is a valiant attempt to standardize business associate language and save legal fees for smaller organizations.
HHS acknowledges that its language is meant merely as guidance and that additional provisions will need to
be added to form a binding contract under state law. However, by now most health plans have had their
attorneys develop standard business associate provisions, so HHS’ guidance would seem to be too late in the
game for most. We’ll have to see whether covered entities will find it practical to use HHS’ sample business
associate provisions.

*Not everybody needs a Business Associate agreement, but some who need a Business Associate agreement don’t know it yet.*

Apparently there is still confusion in the health care industry about under what circumstances a business
associate agreement is necessary. Our organization has received quite a number of business associate
contracts from provider organizations or hospitals, despite the fact that we do not perform any activities on
their behalf. We are educating these providers by identifying the parts of the Privacy Rule and the Preamble
that speak to this issue.

On the other hand, there are probably a lot of vendors out there that will be shocked to receive a 3-page
business associate amendment to their short-form contracts. There has not been much media coverage of the
far, indirect reach of the Privacy Rules, nor of the reality that vendors and service providers in the health care
industry will need to implement new protections of health information via a business associate contract. As
we approach the HIPAA compliance date, vendors who only currently dabble in the health care industry may
likely exit rather than spend the money to implement the Privacy Rules’ business associate protections.

*With apologies to Martha Stewart, it is a “good thing” to offer your own Business Associate agreement but be flexible.*

A standard tactic in negotiating contracts is to get your own contract language out there first. You are more
likely to get the language you want if you initially offer your own language. The same principle holds true with
business associate agreements. For a subrogation company to offer business associate provisions to
prospective health plan clients shows that the company is proactive, aware of the Privacy Rules and willing to
assist the client in its onerous HIPAA compliance tasks. Additionally, a subrogation company offering its
own version of business associate provisions means that it can suggest alternative interpretations of fairly
debatable provisions. If the client has not previously thought of the issue in the way you suggest, perhaps the
health plan client will be persuaded to adopt your different, but equally reasonable, view.

On the other hand, some health plans will be adamant about using their standard business associate
amendment; they will not want to incur legal fees to have their attorneys review an alternative form.
Moreover, state law may require some of the standard business associate provisions to change. For example,
in Wisconsin a statute requires a shorter timeframe for providing individual access to protected health
information. XIII Subrogation companies will therefore want to be flexible about imposing their business
associate provisions upon health plan clients.

*Few agree on the impact of state laws.*
As mentioned above, HIPAA Privacy preemption allows contrary and more stringent state laws to apply. The Privacy Rules define “more stringent” in six different contexts, depending on the type of activity involved.

There is no real industry-wide consensus yet on which state laws are contrary and more stringent and there may never be, absent guidance from HHS. Some trade organizations, like the Health Insurance Association of America (HIAA) and the Blue Cross Association, have offered their members a state law preemption analysis program, but other trade associations have not. Reasonable organizations and even reasonable legal counsel can differ in their interpretations.

One way that a subrogation organization can gain a measure of control over the vagaries of differences in state law interpretation is to include a Preemption clause in their business associate agreements similar to the following:

**Preemption.** To the extent that state law (including statutes, regulations, precedential case law, constitutional provisions and Attorneys General opinions) is saved from preemption under the criteria established in 45 C.F.R. §§ 160.202 and 160.203 (2000), if CLIENT intends Business Associate to comply with state laws (other than the state [where Business Associate is located]) saved from preemption, CLIENT must furnish Business Associate with evidence of any such state laws before Business Associate will be under a duty to comply with such state laws.

Similarly, a subrogation company can and should ask its health plan clients to supply it with HIPAA-compliant authorizations that incorporate relevant state law provisions.

**No one has yet figured out how to predict easily and quickly which state's laws will apply.**

When a person lives, works and receives medical care in the same state where their health insurer is also located, application of state law is simple. In the real world, the planets do not always align so neatly: people do not always live in the same state that they work; they do not always receive medical care in the same state; their health insurer is not always located where they live and work. Application of state law may depend upon all of these factors, depending on how the state law is worded.

The health care industry and the legal community serving it have yet to determine how a multi-state organization can quickly and easily abide by contrary-and- more-stringent state laws. It simply is not practicable (nor cost-effective) to consult attorneys, even in-house counsel, in every multi-state situation. Yet, to follow only the most stringent state laws may result in competitive disadvantage in states with more lenient laws. Most health plans will likely do a risk analysis and comply with the laws in the states in which they do the most business. Subrogation companies could consider adopting the same strategy.

**Conclusion**

In its press release concerning the recent Privacy Rule modifications, HHS promises to conduct outreach and education on the Privacy Rules, including developing fact sheets, handbooks and responding to frequently asked questions. HHS also promises to hold national educational conferences in fall 2002 to address key Privacy Rules issues. The health care industry hopes that HHS is able to provide practical guidance on many of these thorny issues in the time remaining before the compliance date.

**ENDNOTES**

II http://www.hhs.gov/ocr/hipaa

III http://www.archives.gov/federal_register/public_inspection/public_inspection_list.html#spec_H


IX Wisconsin Statutes §610.70(3) and (4) (2000).

X 45 C.F.R. §164.504(e)(2)(ii)(E).


XIII Wisconsin Statutes § 610.70(3) (2000) requires an insurer to provide an individual access to personal medical information within 30 days, rather than within 30 days with one available 30-day extension as allowed under the Privacy Rules, 45 C.F.R. § 164.524(b)(2)(i) and (iii).

XIV 45 C.F.R. §160.202 (as modified by the Privacy Rule modifications issued August 14, 2002) defines a “more stringent” state law as:

(1) Prohibiting or restricting a use or disclosure that would otherwise be permitted by the Privacy Rules (unless the disclosure is required by the HHS Secretary to determine compliance, or is to the individual that is the subject of the PHI);

(2) Permitting greater rights of access or amendment of PHI;

(3) Providing greater amount of information to the individual about use, disclosure, rights and remedies;

(4) Narrowing the scope or duration of, increasing the privacy protections afforded to, or reducing the coercive effect of authorizations;

(5) Providing for the retention or reporting of more detailed information or for a longer duration (relating to disclosure accounting); or

(6) Providing greater privacy protection to the individual.

XV For more information on the Preemption program available to members of the Health Insurance Association of America, American Association of Health Plans and the Blue Cross Blue Shield Association, contact Attorney Bruce Fried at the law firm of Shaw Pittman LLC, at bruce.fried@shawpittman.com.