

HIPAA liability: Beware the secondary enforcers

Daniel L. Icenogle, MD, JD

HIPAA compliance is upon us. Having passed the long awaited April 14, 2003 enforcement date, we have all become familiar with the notices of privacy practices and other manifestations of compliance with HIPAA, the Health Insurance Portability and Accountability Act of 1996. Some time in the next few months, we will also begin to see examples of HIPAA enforcement. There will be HIPAA complaints and investigations; there will be enforcement actions by the Office of Civil Rights (OCR), the HIPAA enforcement agency. But there will also be innovative efforts by plaintiff's attorneys to obtain judgments against physicians and hospitals based on HIPAA violations, something obviously not envisioned by HIPAA.

As we looked forward to HIPAA enforcement, we saw that the language of HIPAA and the various guidance documents that have come from OCR indicated an almost warm and fuzzy attitude toward compliance enforcement, as long as reasonable efforts were being made. Granted, while there was no question that the ramifications of complete disregard for compliance

would be significant, there is in the HIPAA regulations and preambles, as well as in statements from OCR personnel, an attitude of assistance and reasonableness that permeates the enforcement mindset.¹ OCR appears committed to offering technical assistance and sufficient time for covered entities to achieve compliance, as long as the efforts made up to the time of an investigation have been reasonable given the nature of the covered entity. As a result, many have counseled clients who were not going to achieve full privacy compliance by last April not to panic, but to continue to work with all deliberate speed towards compliance. And, in fact, a high percentage of covered entities did fail to achieve full privacy compliance by April 14. In a Health Information Management Systems Society (HIMSS)/Phoenix Health Systems survey from early April, self-reported privacy compliance for providers was only 78%.² It was even lower for health plans (68%) and very low for clearinghouses (47%). One basis for clearinghouses' poor percentage may be that, with the Transaction and Code Set Rules not due for compliance until October, 2003, clearinghouses were more like business associates and not-yet-covered entities.

Reasonable Efforts

While there is no general rule that only reasonable efforts are needed

to meet the privacy regulations or to be in compliance, the term is used frequently throughout the regulations. The absence of a specific definition precludes a provider from asserting that only a reasonable effort to comply with HIPAA will be sufficient to avoid any complaints about such compliance. Instead, the presence of the "reasonableness" gloss should be noted and can be useful, but only within the context of the specific section of the regulation.

For example, while the regulations generally require that a provider discontinue a relationship with a business associate in a case of breach of privacy by that business associate, the regulations do allow a provider to continue to use the same business associate if it is not reasonable to do otherwise. Here it is only reasonable to continue to use the business associate if it is impossible to replace, but not if it is simply inconvenient or more expensive to use another.

On the other hand, in other contexts a reasonableness standard may include economic considerations. The Secretary of Department of Health and Human Services, former Wisconsin Governor Tommy Thompson, has written that there is an expectation that the requirements of the final rule will not be difficult to fulfill. This seems to express the hopeful view that there is no expectation that compliance will

Doctor Icenogle is an emergency medicine physician, as well as a health law attorney with Icenogle and Associates, LLC. He can be contacted at S7563 Riley Rd, Readstown, WI 54658; phone 608.675.3000; e-mail dicenogle@icenogle.net.

require complex or expensive efforts that could endanger the existence of a small provider.

Flexibility/Scalability

In addition to an attitude of reasonableness towards enforcement, there is no question that the final privacy regulations emphasize an inherent flexibility or scalability to meet the needs of different sized entities. The concept of scalability is repeated in the OCR's Privacy Guidance document, which outlines OCR's attitude towards various issues raised by HIPAA. However, while the language is encouraging, there are very few specific examples of how that sense of scalability is to be put into practice. Instead, there are only general themes. One important recurring theme is that HIPAA is not meant to introduce dramatic change to the business practices of providers as long as the spirit of HIPAA is honored. The August 2002 modifications to the privacy rule demonstrate that commitment by removing much of the regulation of areas that seemed to present little risk of privacy loss.

HIPAA Lawsuits

However, no matter how reassuring all of this may be, OCR may not be the only HIPAA "enforcer" that covered entities need to be concerned about. The other possibility is that trial lawyers may try to find opportunities to use HIPAA standards as the basis for lawsuits against physicians and other covered entities. Indeed, there has always been some concern that creative attorneys may fashion legal arguments that attempt to turn a HIPAA violation into a violation of state law. However, HIPAA itself provides no basis for an individual to sue a covered entity for a HIPAA violation; that is, there is no private right of action under HIPAA. The sole

avenue open under HIPAA for an individual who feels aggrieved by a HIPAA violation is for that person to file a complaint with OCR. OCR will then investigate the complaint, and OCR alone will enforce any violation of HIPAA standards. However, that does not mean that there are not opportunities for direct legal action by an individual patient against a physician or hospital based on an alleged HIPAA violation. To pursue legal action, an individual would have to convince a court that the HIPAA violation either breached a standard of care or violated a state statute. There are two ways this can happen. One, HIPAA is held to have created a standard of practice for covered entities, or two, a state law has been written in such a fashion that a HIPAA standard would become a standard of behavior required by the state law.

The latter would seem to be an unlikely task. Typically, state confidentiality laws, which often do create a private right of action, fully define what is meant by a breach of confidentiality and it is not likely that any HIPAA standard could enter into the definition. Moreover, state confidentiality laws are preempted by HIPAA unless they are more stringent, and a HIPAA violation would be unable to implicate a parallel state law if that state law has been preempted by HIPAA. If state law survives HIPAA preemption by being more stringent, any HIPAA violation would likely violate state law in its own right, with its own enforcement provisions operating regardless of HIPAA's existence. That said, at least one state, Texas, has adopted new confidentiality laws that specifically adopt HIPAA standards, making them applicable to areas in which HIPAA itself may not be. But even in this case the state law would operate independently.

It is the strategy that HIPAA would be held to have created a standard of practice for covered entities that will likely be used by the plaintiffs' bar to attempt to find liability from a HIPAA violation. In this scenario, the argument will be that HIPAA is setting a national standard of care for patient confidentiality and any failure to meet that standard must then be a breach. Arguing using medical malpractice or other state law theories, it is inevitable that plaintiffs will attempt to create liability for HIPAA violations. And, in fact, it has already happened.

The Hospice Patients Alliance, a Florida advocacy group, has filed what may have been the first HIPAA complaint in the country with OCR, reporting alleged violations by a hospice organization in Florida, the Hospice of the Florida Suncoast. The case began in February 2003 with the filing of a class action lawsuit in Florida state court alleging that the hospice illegally diverted donated funds in order to purchase a software company and manage it as a for-profit subsidiary, Suncoast Solutions. This subsidiary hoped to sell hospice-specific computer software to other hospices on a nationwide basis. On May 1, 2003, a second lawsuit was filed, alleging that the hospice and Suncoast Solutions disclosed real patients' health data in its software marketing and promotions, as well as in the help screens and elsewhere throughout the software itself. This allegation formed the basis of the OCR complaint: that the hospice violated HIPAA by disclosing protected health information without an authorization for marketing purposes. In addition to the OCR complaint, the Alliance has argued in this second lawsuit that these disclosures violate state law. Documents that could further delineate the state law

theories behind this second lawsuit are not generally available at this time.

This case does clearly point out that the plaintiffs' bar is aware of HIPAA and is capable of trying to creatively use state law to attempt to bring a HIPAA violation into the courtroom. While the likelihood of success in this sort of lawsuit remains unknown, the reward for success may be great. In a pre-HIPAA case, a Morgantown, WV jury awarded \$2.3 million in February 2003 to three women whose mental health treatment records were not kept private by West Virginia University Medical Corporation. The awards included \$766,200 to one woman, \$762,000 to another and \$750,000 to the third. Their injuries were, of course, only to their reputations, based on the exposure of the fact that they had been treated for mental health disorders. The value of that sort of injury is a question for the jury, and at least one jury obviously placed a very high value on it.

Regardless of the success of any HIPAA-based lawsuit, cases such as these will receive attention in the media, causing patients to become increasingly more aware of their privacy. Physicians, hospitals and other covered entities must remain acutely cognizant of this growing awareness. In addition to meeting the terms of HIPAA compliance, physicians must cultivate a culture of privacy within their clinics in order to meet something even more important: the expectations of their patients.

References

1. Office of Civil Rights HIPAA Privacy Rule enforcement guidance found at www.hhs.gov/ocr/hipaa/privacy.html.
2. HIMSS/Phoenix Health Systems survey reported at www.hipaadvisory.com/action/surveynew/Spring2003.htm.

Wisconsin Medical Journal

The mission of the *Wisconsin Medical Journal* is to provide a vehicle for professional communication and continuing education of Wisconsin physicians.

The *Wisconsin Medical Journal* (ISSN 1098-1861) is the official publication of the Wisconsin Medical Society and is devoted to the interests of the medical profession and health care in Wisconsin. The managing editor is responsible for overseeing the production, business operation and contents of *Wisconsin Medical Journal*. The editorial board, chaired by the medical editor, solicits and peer reviews all scientific articles; it does not screen public health, socioeconomic or organizational articles. Although letters to the editor are reviewed by the medical editor, all signed expressions of opinion belong to the author(s) for which neither the *Wisconsin Medical Journal* nor the Society take responsibility. The *Wisconsin Medical Journal* is indexed in Index Medicus, Hospital Literature Index and Cambridge Scientific Abstracts.

For reprints of this article, contact the *Wisconsin Medical Journal* at 866.442.3800 or e-mail wmj@wismed.org.

© 2004 Wisconsin Medical Society