

HIPAA Privacy and Security Enforcement: Assessing and Reducing Risks

Andrew B. Wachler, Esq.

Amy K. Fehn, Esq.

As of April 14, 2003, covered entities are expected to be in compliance with the HIPAA Privacy Rule and the April 21, 2005 deadline for Security is rapidly approaching. Health care providers and their attorneys are now left wondering where the liability risks lie and how to best mitigate these risks.

Governmental Enforcement of the Privacy Rule

The Interim Final Enforcement Rule, published on April 17, 2003, reaffirms the government's previous statements that HIPAA enforcement will be primarily complaint driven.¹ According to the Office of Civil Rights, as of early September, the office has received over 1760 HIPAA complaints. Of these 1760 complaints, 500 have been closed and 1260 remain open for investigation. This number is relatively low in light of the number of covered entities that are subject to HIPAA and, therefore, seems to suggest that the risk of governmental investigation is also relatively low.

The Interim Final Enforcement Rule also reaffirms the Department of Health and Human Services' commitment to provide technical assistance and promote voluntary compliance when investigating HIPAA complaints. In addition, covered entities have statutory defenses available to avoid imposition of civil monetary penalties where the covered entity did not know of the violation, or through the exercise of reasonable diligence would not have known of the violation. In addition, if a violation is due to "reasonable cause" and not "willful neglect" and the violation is corrected within thirty days, civil monetary penalties will not be imposed. The DHHS has discretion to extend this thirty day correction period or to reduce or waive a civil monetary penalty if the "payment of such penalty would be excessive relative to the compliance failure involved."² Thus, even if a complaint were to occur, most covered entities will not be faced with civil monetary penalties if they have acted in good faith.

According to the Office of Civil Rights, at least some of the complaints received to date have been forwarded to the Department of Justice for criminal investigation. However, criminal penalties will be reserved for knowing violations. Penalties increase for those violations committed under false pretenses, for commercial advantage, personal gain or malicious harm.

Private Causes of Action for Breach of Privacy

With respect to negligent disclosures of protected health information, private litigation may be the biggest risk that covered entities will face. Even before the deadline for compliance with the Privacy rule, plaintiffs' attorneys have successfully brought suits

¹ 68 Fed. Reg. 18895.

² 42 U.S.C. 1320d-5.

against health care providers for breaches of patient confidentiality through various causes of action. Although the HIPAA statute does not create a private cause of action, most attorneys agree that it will likely be used to create a duty to safeguard medical information and to establish a national standard of care among the medical community.

A recent Michigan case demonstrates the way in which a confidentiality statute can be used to establish a private cause of action. In *Doe v. American Medical Pharmacies, Inc.*³, a pharmacy employee loudly blurted a patient's HIV status in a crowded waiting room. The court of appeals upheld a jury verdict of \$100,000 for slander, invasion of privacy, intentional infliction of emotional distress, and violation of a Michigan statute that protects the confidentiality of HIV results.⁴ Like HIPAA, the confidentiality statute allows for fines and/or criminal sanctions, but does not create a private cause of action. Similarly, a 1991 case from Michigan recognized that the psychiatrist/patient privilege statute and the confidentiality portions of the medical licensing statute create a legal duty. Although the statutes do not create a private cause of action, the failure of a psychiatrist to comply with these statutes was considered by the court to be a breach of the legal duty, and, therefore, actionable as medical malpractice.⁵

A mental health confidentiality statute was also used in a West Virginia case against West Virginia University Medical Corporation resulting in a 2.3 million dollar jury verdict. Again, the statute did not create a private cause of action, but was successfully used to establish a provider's legal duty. The plaintiffs in this case were three mental health patients whose information was disclosed in a bar by a records clerk.⁶

Other courts have found a duty of confidentiality even in the absence of a statutory obligation. For example, a Washington, D.C. jury entered a \$250,000 verdict against a hospital for failing to adequately safeguard a patient's medical records when a temporary receptionist accessed the record and informed the patient's co-workers of the patient's positive HIV status. In this case, the court recognized a health care providers' legal duty to protect confidential information, basing this duty on the common law tort of "breach of confidential relationship." The court further noted that the hospital-patient relationship was customarily understood to carry an obligation of confidence.⁷

In addition to negligence and medical malpractice actions, other courts have used statutorily created causes of action, such as the tort of invasion of privacy. For example, in the Wisconsin case of *Pachowitz v. LeDoux*, a volunteer fire department was held liable when an emergency medical technician discussed a patient's medical information with one of the patient's co-workers. The plaintiff relied upon a statute that creates a cause of action for compensatory damages and attorney fees where the plaintiff proves that a defendant acted unreasonably or recklessly in making a public disclosure of private

³ *Doe v. American Medical Pharmacies, Inc.* (unpublished), 2002 WL 857766 (Mich. App.).

⁴ MCLA 333.5131.

⁵ *Saur v. Probes, M.D.*, 190 Mich. App. 636.

⁶ See Judge's Charge to Jury in the case of *CLA, MC and JP v. W. Va. Univ. Med. Corp.*, Circuit Court of Monongalia County, West Virginia, Division No. 2, Civil Action No. 99-C-509 and West Virginia Code §27-3-1.

⁷ *Doe v. Medlantic Health Care Group* (2001), 814 A.2d 939.

facts about the plaintiff that would be highly offensive to a reasonable person of ordinary sensibilities.⁸

These cases demonstrate the willingness of the courts to award damages for breaches of patient confidentiality. This willingness, combined with the ability to use HIPAA as a national standard of care, will likely make it easier for plaintiff's attorneys to bring such cases in the future.

Private Causes of Action for Security Breaches

Although compliance with the Security Rule is not technically required until April 21, 2005, the Privacy Rule requires covered entities to maintain "appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information."⁹ Security breaches are especially risky because one breach can impact numerous patients. For example, in December 2002, computers containing health information on 562,000 individuals were stolen from TriWest Healthcare Alliance, a health care contractor for military personnel. The theft resulted in a class action lawsuit against TriWest.¹⁰

Reducing Risks

Although it is impossible to completely eliminate the risk of privacy or security breaches, there are steps that attorneys can take to assist covered entities with reducing risks of liability from both a governmental enforcement and a private litigation standpoint. Many of the cases discussed above resulted from the negligent or intentional acts of the covered entities' employees. An effective employee training program and disciplinary policy would help to reduce the risk of these types of occurrences. For this reason, the goal of employee training programs should go beyond the HIPAA training requirements, which are quite vague. Attorneys should assist their clients in setting up comprehensive and ongoing training programs that will actually effectuate compliance with privacy policies. In addition, it is important that employees be disciplined appropriately for noncompliance.

Documentation of the decision making process is also very important for risk reduction. Both the privacy rule and the security rule allow covered entities to make decisions regarding which safeguards are "reasonable and appropriate" for their environment. If a particular safeguard is not implemented because it would impede patient care or would create an unreasonable financial burden for the organization, the reason for the decision should be well documented. This documentation may be needed to defend a government enforcement action or a private lawsuit and should be carefully drafted with counsel's assistance in a manner that would be helpful in this context.

⁸ Pachowitz v. LeDoux, 666 N.W.2d 88 (2003).

⁹ 45 CFR 164.530(c)(1).

¹⁰ Dennis Wagner, "Lawsuit Accuses TriWest Health Care of Negligence", The Arizona Republic, January 30, 2003.

Certain documentation may hurt a provider's ability to defend litigation, but is nevertheless required by the HIPAA Privacy Rule or Security Rule. For example, the Privacy Rule requires covered entities to investigate and document the results of all patient complaints and employee disciplinary actions related to HIPAA. The Security Rule requires covered entities to conduct a risk analysis, documenting all potential risks and vulnerabilities of its electronic protected health information. This information must be disclosed to the government upon request and should be drafted with this in mind. In a lawsuit, this information could be used to demonstrate that a provider knew of a risk or a pattern of conduct by its employees and failed to take adequate actions. Attorneys who represent covered entities should explore ways of protecting drafts of reports to the extent possible under either the attorney client privilege or as attorney work product.

Attorneys could also assist covered entities with HIPAA compliance by performing internal "audits" of the covered entity's privacy and security policies and practices. Because such internal audits are not required by HIPAA, the findings would not have to be disclosed to the government and could be protected by the attorney client privilege. The audit could be used as a valuable tool to alert clients of potential problems before they are faced with a patient complaint, government investigation, or lawsuit.