

HIPAA Privacy and Security Enforcement: Recognizing and Reducing Risks

Andrew B. Wachler, Esq.

Amy K. Fehn, Esq.

With the passing of the HIPAA Privacy Rule deadline and the Security Rule deadline looming, many covered entities are left wondering if they are doing enough to prevent privacy and security breaches and what type of exposure their organization could face in the event of a breach.

Government Enforcement

The Interim Final Enforcement Rule, published on April 17, 2003, reaffirms the government's previous statements that HIPAA enforcement will be primarily complaint driven. 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.

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."

HIPAA's criminal penalties, which will be addressed in the second installment of the enforcement rule, will be reserved for knowing violations. Penalties increase for those violations committed under false pretenses, for commercial advantage, personal gain or malicious harm. 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.

Litigation Risks

Negligent or intentional disclosures of protected health information also create a litigation risk. Although the HIPAA statute does not create a private cause of action, it may establish a duty or standard of care for health care providers. When damages ensue as a result of a breach of the duty or standards, patients could sue the provider under numerous legal theories, such as negligence or breach of privacy.

In the 2002 Michigan case of *Doe v. American Medical Pharmacies, Inc.*, a patient successfully sued a pharmacy for \$100,000. The basis of the suit was slander, invasion of

privacy and intentional infliction of emotional distress resulting from an employee loudly blurting the patient's HIV status in a crowded waiting room. Similar cases have arisen in other states, including a West Virginia case where the jury awarded 2.3 million dollars to three mental health patients whose information was disclosed in a bar by a records clerk. In Wisconsin, 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. 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.

Although compliance with the Security Rule is not technically required until April 21, 2005, the Privacy Rule and the HIPAA statute require covered entities to "maintain appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 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 was stolen from TriWest Healthcare Alliance, a health care contractor for military personnel. The theft resulted in a class action lawsuit against TriWest.

Reducing Risks

Although it is impossible to completely eliminate the risk of privacy or security breaches, there are steps that covered entities can take to reduce risks of liability from both a governmental enforcement and a private litigation standpoint. An effective employee training program and disciplinary policy will reduce risks significantly. While privacy policies are important, they can actually cause more harm than good if employees are not appropriately trained and disciplined 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 in a manner that would be helpful in this context.

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. Providers

should work closely with counsel to protect drafts of reports to the extent possible under either the attorney client privilege or the attorney work product privilege.

As with other areas of compliance, a HIPAA compliance program will not be effective if it is not actively maintained. Providers can significantly reduce the risk of a government investigation or a civil lawsuit by offering frequent employee training programs and closely monitoring compliance with privacy and security policies.