

# New Jersey Law Journal

VOL. CLXXXI—NO. 12—INDEX 1089

SEPTEMBER 19, 2005

ESTABLISHED 1878

IN PRACTICE

## HEALTH CARE LAW

By SIMONE HANDLER-HUTCHINSON

### Is the Worst Yet To Come?

HHS and the courts are finally talking about HIPAA enforcement

Compliance with the myriad of privacy, security and electronic transaction standards promulgated under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) is now a reality for most health care entities. The compliance dates for the HIPAA Privacy Rule, Electronic Transactions Rule and Security Rule were April 2003, Oct. 2003, and April 2005, respectively (except for small health plans). Health care entities covered by the HIPAA rules, which include health care plans, health care clearinghouses, health care providers that submit electronic transactions and Medicare prescription drug card sponsors have had ample time to digest and attempt to implement HIPAA's extensive and often inexact compliance requirements. But the question of civil and criminal HIPAA enforcement remains: will the government really punish organizations for HIPAA violations or will the Department of Health and Human Services (HHS) continue promoting its

friendly approach of voluntary HIPAA compliance through education, guidance and technical assistance? While there has already been one major criminal conviction for a HIPAA violation thus far (summarized below) the enforcement message remains mixed. For example, while thousands of privacy complaints have been filed with and investigated by the HHS Office for Civil Rights (OCR) and the agency has been given authority to administer and enforce the HIPAA Privacy Rule, no civil penalties have been imposed. At the same time, HHS has recently issued a proposed enforcement rule setting forth, among other things, the process for imposing civil monetary penalties for HIPAA violations. In addition, state and federal courts are increasingly addressing HIPAA in a wide variety of factual contexts. What follows is a summary of where these HIPAA enforcement activities are heading.

#### Privacy Complaints Roll In

Speaking unofficially at a recent national conference, an OCR representative reported that over 14,900 privacy complaints had been received, and that approximately 70 percent had been resolved or closed. The representative further reported that approximately 80 percent of complaints are investigated.

The remainder are not investigated due to one of the following reasons: 1) the conduct complained of occurred prior to the HIPAA Privacy Rule compliance date; 2) the person or entity complained of is not a covered entity; or 3) the conduct complained of does not violate HIPAA.

Although the factual bases supporting these privacy complaints vary widely, OCR indicated that many of them could be grouped into a few general categories, such as: 1) alleged improper uses or disclosures of protected health information (disclosing information without patient authorization, oral discussions in public areas); 2) alleged inadequate or nonexistent privacy safeguards (leaving medical records or computer screens in plain view); 3) access to or copies of protected health information allegedly denied or delayed; 4) alleged disclosure of more information than needed (failure to adhere to the "minimum necessary" rule); and 5) failure to include required language in patient authorizations. Though many different types of covered entities have been the subject of the privacy complaints received by OCR, private health care providers, such as doctors and dentists, have received more complaints than other types of organizations. They're followed by hospitals, pharmacists, outpatient facilities, and group health plans. With regard to criminal conduct, OCR indicated that over 200 privacy complaints of a criminal nature have been referred to the Department of Justice (DOJ) for further investigation and possible criminal prosecution.

---

*Handler-Hutchinson is a member of the health law practice group of Schenck, Price, Smith & King of Morristown. Her practice is devoted to the legal, regulatory and compliance issues facing hospitals, physicians and other health-care professionals and entities.*

### First Criminal Conviction

Richard W. Gibson, a lab employee of a Seattle, Wash. hospital was found guilty of violating the HIPAA privacy law. Gibson used a cancer patient's personal identifying information to obtain credit cards in the patient's name and then charged over \$9,000 in purchases. In August 2004, Gibson pleaded guilty in federal court to wrongful disclosure of individually identifiable health information for economic gain. Gibson ultimately signed a plea agreement and in Nov. 2004, a judge sentenced Gibson to 16 months in jail, three years of supervised release, and monetary restitution for wrongful disclosure of confidential patient information. The District Court Judge sentencing Gibson told him, "your behavior in this case is some of the most deplorable I've seen in 15 years on the bench." This is the first criminal conviction under HIPAA. The plea agreement is available online at the U.S. Attorney's office: [www.usdoj.gov/usao/waw/press\\_room/2004/au\\_g/pdf\\_files/cr04\\_0374rsm\\_plea.pdf](http://www.usdoj.gov/usao/waw/press_room/2004/au_g/pdf_files/cr04_0374rsm_plea.pdf)

### DOJ Issues HIPAA Opinion

Less than a year after Gibson's conviction, on June 1, 2005, the Department of Justice, Office of Legal Counsel, issued a memorandum opinion on the scope of criminal enforcement under 42 U.S.C. § 1320d-6 of HIPAA. The opinion was issued in response to questions posed by the HHS' general counsel. The opinion appears to undercut the Gibson conviction.

The memorandum opinion addressed the following issues:

1) Whether the only persons who may be directly liable for HIPAA criminal enforcement are those persons to whom the substantive requirements apply — i.e., health plans, health care clearinghouses, certain health care providers and Medicare prescription drug card sponsors — or whether others may be directly liable, particularly someone who causes a person, who is otherwise subject to the substantive

requirements of HIPAA, to release protected health information in violation of that law.

2) Whether the "knowingly" element of the HIPAA statute requires only proof of knowledge of the facts that constitute the offense or whether this element also requires proof of knowledge that the conduct was contrary to the statute or regulations.

Section 1320d-6(a) states:

A person who knowingly and in violation of this part:

1) uses or causes to be used a unique health identifier;

2) obtains individually identifiable health information relating to an individual; or

3) discloses individually identifiable health information to another person, shall be punished as provided in subsection (b) of this section. 42 U.S.C. §1320d-6(a).

Penalties for the above violations include monetary fines up to \$250,000 and up to ten years in prison, punished as provided in subsection (b) of this section. 42 U.S.C. §1320d-6(b).

In response to the first question, the DOJ opinion limits the criminal applicability of the statute by concluding that only covered entities (i.e., health plans, health-care clearinghouses, certain health-care providers and Medicare prescription drug card sponsors) may be subject to criminal prosecution for violations of 1320d-6. While the opinion also adds that in certain factual scenarios, it is possible for certain individuals such as directors, officers and employees of covered entities to be subject to criminal prosecution under section 1320d-6, it states that others — such as noncovered entities — may not be directly liable. The opinion goes on to state that the liability of others may instead "be determined by principles of aiding and abetting liability and of conspiracy liability."

In response to the second question, the opinion addresses the "knowingly" element of the offense. The opinion

states, to "incur criminal liability, a defendant need have knowledge only of those facts that constitute the offense." HIPAA does not also require "proof of knowledge that the conduct was contrary to the statute or regulations."

### Proposed Enforcement Rule

On April 18, HHS published in the *Federal Register* a proposed rule on HIPAA enforcement. Fed. Reg., Vol. 70, No. 73 (04/18/05), p. 20224. Significantly, the proposed enforcement rule governs compliance with and enforcement of all HIPAA Administrative Simplification rules — including the Privacy Rule, Security Rule and Electronic Transactions Rule and sets forth the process for investigations of noncompliance with those rules. In the preamble to the proposed rule, HHS stated as its general approach that it is "committed to promoting and encouraging voluntary compliance with the HIPAA rules through education, cooperation, and technical assistance." Fed. Reg., Vol. 70, No. 73 (04/18/05), at 20226. HHS also confirmed that its HIPAA compliance efforts are often complaint driven. While OCR administers and enforces HIPAA Privacy Rule compliance, the Centers for Medicare & Medicare Services (CMS) has been delegated with the authority to administer and enforce all nonprivacy HIPAA rules.

The proposed enforcement rule sets forth the process for the conduct of investigations, compliance reviews and includes the imposition and calculation of civil monetary penalties for HIPAA violations by covered entities. In the event that a penalty is assessed, HHS is required to provide the covered entity with written notice of HHS' intent to impose a penalty. The notice must include, among other things, the basis for such penalty, the amount of the penalty and a statement of the covered entity's right to request a hearing before an administrative law judge (ALJ). The proposed rule also describes the procedural aspects of such hearings, including authority to settle, conduct of dis-

covery, fees and appeals from the ALJ decision.

### Courts Weigh In

The courts are increasingly addressing HIPAA in a variety of state and federal cases with diverse factual and procedural contexts. These decisions have tackled such topics as HIPAA pre-emption of state law, the right to request protected health information in the course of legal proceedings and disputes between providers over medical records. For example, a recent New Jersey appellate division case addressed the HIPAA Privacy Rule. *Michelson v. Wyatt*, unpublished, N.J.L.J. DDS No. 52-2-1217 (App. Div., 8/11/05). The plaintiff, a Plainfield resident, requested health insurance benefits information of Plainfield city employees under the Open Public Records Act (OPRA). Some of the documents were requested from the State Health Benefit Commission, which administers the

health insurance plan for the city. The city produced only some of the documents and the plaintiff filed a complaint requesting the unproduced documents. The lower court dismissed the complaint, holding that the records were exempt from OPRA and were otherwise protected under state and federal law. On appeal, the court affirmed that the documents were not government records subject to disclosure under OPRA. The court further held that the Commission was a covered entity under the HIPAA privacy rule and HIPAA and New Jersey law were consistent on this issue and as such, disclosure of the records was not permitted.

In a New York case, a dentist leaving a dental practice sought from his former dentist partners all the patient records of the practice. *Lewis v. Clement*, 1 Misc. 3d 464 (N.Y. Misc. 2003). The dentist had already received records for patients he had treated while he was a partner. The court held the patient records were the property of the treating physician or

physicians and that when the partnership dissolved, the dentist was entitled only to those records of patients with whom he had a direct treatment relationship.

And in a Colorado case, a hospital filed a complaint against a newspaper publishing company, claiming that the company's use and publication of a peer review report, obtained from an anonymous source, violated HIPAA. *Univ. of Colo. Hosp. Auth. v. Denver Publ. Co.*, 340 F. Supp.2d 1142 (D. Colo. 2004). The court held that the hospital did not have a private right of action under HIPAA. The court noted that § 1320d-6(b)(3) provided a statutory penalty for entities that obtained or disclosed individually identifiable health information; however, there was nothing set forth in any HIPAA provision that conferred privacy rights upon any entity or identified any intended beneficiary. The court granted the company's motion to dismiss the claim under HIPAA and remanded the remaining claims to state court. ■