New York Law Journal
SERVING THE BENCH AND BAR SINCE 1888
Web address: http://www.law.com/ny
MONDAY, JULY 2, 2001

HEALTH CARE LAW

HIPAA Regulations' Unintended Effect

Civil Actions for Inappropriate Disclosure of Patients' Medical Information May Increase

BY RONALD J. LEVINE AND ANNE MALTZ

THE RIGHTS AND responsibilities created pursuant to the Health Insurance Portability & Accountability Act of 1996[1] (HIPAA) will change the nature of how a patient's medical information is handled and disclosed by all entities that have access to this information. HIPAA creates a new standard for the management of patient information. The regulatory requirements for implementation are highly complex and will require a significant expenditure of resources by affected parties such as health care providers and health insurance plans.

An unintended effect of the new regulations is the likelihood that the incidence of civil litigation brought for an inappropriate disclosure of a patient's medical information will increase. This article will explore the basic requirements of HIPAA, the causes of action that health care providers can anticipate will result, and finally, what health care providers, health plans and their associates can do to avoid costly litigation.

Patient Privacy Rights

The final regulations for maintaining the privacy of medical information became effective on April 14, 2001.[2] Compliance is required for most covered entities by April 14, 2003. In general, the privacy regulations limit covered entities' rights to use or disclose protected health information. Covered entities include health care providers (doctors, hospitals, nurses, nursing homes, etc.), health plans (payors such as HMOs, self-insured funds, etc.), health care clearinghouses (a type of claim processor) and their business associates.

The regulations create broad protections and new rights with regard to a patient's protected health information (PHI). While the privacy regulations do not provide for a federal cause of action, they do set the stage for making civil litigation based on the improper disclosure or use of health information easier and, therefore, more frequent. In order to understand the increased potential for litigation, a brief overview of the new privacy rights and responsibilities set forth in the regulations is necessary.

HIPAA establishes five patient rights with respect to use and disclosure of PHI:

• *Notice*. Individuals have a right to notice of (a) the uses and disclosures of their PHI by the covered entity; (b) their individual rights; and (c) a covered entity's legal duties.

• *Access*. Individuals have the right to access, inspect and copy their records.

• *Amendment*. Individuals have the right to request that the covered entity amend their PHI.

• *Additional Restriction*. Individuals may request additional restriction of the covered entity's use and disclosure of their PHI. The covered entity need not agree to grant such request.

• *Accounting*. Individuals have the right to receive an accounting of a specific class of disclosures of PHI made by a covered entity during the preceding six years.

In addition to these specific rights, the regulations require written consent of the individual before PHI may be disclosed for purposes of treatment, payment or health care operations. Indeed, most disclosures, except in an emergency, for government oversight or public health purposes, or in some cases, for research, require the disclosure to be authorized in writing by the subject of the information. Additionally, except where disclosure is required for treatment, is made to the patient or is required by law, only the "minimum necessary" amount of information may be disclosed.

The impact of these changes and others is significant and will require a change in the culture of handling medical information at

every level within a covered entity. Policies and procedures will have to be implemented to enable compliance with the new regulations. While covered entities work out these compliance procedures, it is easy to imagine intentional and unintentional breaches of patient privacy rights that could lead to disclosures prohibited by the HIPAA privacy regulations.

When faced with such a disclosure, the patient has different paths he or she can choose to address the problem. The patient can file a complaint with the covered entity's complaint officer. In the alternative, the patient can file a complaint with the U.S. Department of Health and Human Services (HHS) which may lead to the levying of civil or criminal penalties by HHS against the alleged violator. The patient may also choose to file a civil lawsuit and use the violation of HIPAA as a basis for proving liability on the part of the covered entity.[3]

HIPAA and Civil Actions

While HIPAA does not in itself provide a cause of action for breach of confidentiality or privacy, the regulations will undoubtedly be offered in private actions to show the minimal standard of care expected of all physicians, hospitals, health care providers and health plans with respect to managing and protecting PHI. In the absence of a common law right to privacy,[4] aggrieved individuals must rely upon contract and tort theories in pursuing their claims. Individuals may also wish to base their claims on applicable New York State statutes.

Weight of the Statute. The weight accorded to HIPAA by the courts will be significant in negligence actions. While New York courts do not uniformly accept or reject federal regulations in assessing the appropriate standard of care or in determining liability, the violation of a state or federal statute has been held to constitute negligence per se in certain circumstances.[5]

Health care providers must also be aware that compliance with the regulations of HIPAA alone may not be sufficient to prevent a cause of action from arising. For example, while the appropriate standard of care is generally determined in terms of industry or business practice, on occasion, the courts have held that nothing less than the best practice or protection was acceptable.[6]

Even HIPAA recognizes that the best practice may not be universal. Policies and procedures designed to comply with the regulations must take into account the size of the covered entity and the type of activities relative to PHI that it undertakes.[7] The practical result of this notion, referred to throughout HIPAA's preamble as "scalability," is that while covered entities are required to implement all of the regulations, implementation is intended to vary with the size and complexity of the covered entity.

Furthermore, HIPAA creates merely a "floor" or base line for protection of medical information. While HIPAA pre-empts state laws that are less stringent than its provisions, it specifically defers to state laws, affording patients greater protection and access to information.[8] In general, preemption will occur unless (1) the Secretary of HHS determines a specific statute falls within a category of exempted state regulatory functions, or (2) the provisions of the state law relate to the privacy of health information and are more stringent than the corresponding standard under HIPAA.

Under HIPAA,[9] a state privacy law which is contrary to HIPAA would be deemed more stringent if it: creates greater rights of access or amendment; provides more information to the patient about use, disclosure rights or remedies; provides more control to the patient over the form or substance of patient authorization and consent; requires retention of records for a longer duration; or provides more privacy protection to the patient.

New York has a fairly comprehensive set of laws and regulations on confidentiality and privacy, some of which may be deemed more stringent. For example, under the HIPAA privacy rules, the subject of PHI has a right to inspect and obtain a copy of his or her PHI. The request must be acted upon by the covered entity within 30 days.[10] In contrast, N.Y. Pub. Health Law §18.2 requires health care providers to allow an individual access to his or her patient information within 10 days of the request. As compliance with a request for information within 10 days is clearly more stringent than compliance within 30 days, §18.2 would apply over HIPAA. However, while a stringency analysis involving days or time is relatively easy to perform, the comparative stringency of other contrasting regulations may not be as easy to decipher.

Causes of Action for Unauthorized Disclosure of Health Information. While tort claims based on negligence and the breach of fiduciary duty have been received more favorably in New York than claims based on breach of contract, suits brought under either theory can result in recovery.[11] Breach of contract claims have been brought against physicians for unauthorized disclosure of patient information to third parties in violation of specific[12] or implied contracts to keep the information confidential.

Indeed, absent a specific agreement between the parties to keep health information confidential, New York courts have recognized that the agreement between a physician and patient for the provision of medical services includes an implied covenant to keep in confidence all disclosures made by the patient concerning his medical condition as well as all matters discovered by the physician in the course of examination or treatment.[13]

However, the majority of cases involving breach of confidentiality claims addresses the cause of action as one of a breach of fiduciary duty owed by a physician to his or her patients to keep medical information confidential, rather than as a breach of contract.[14] One reason for this preference is that the types of damages incurred by plaintiffs in these actions can be addressed more appropriately under tort law than under contract law.

A plaintiff suing for breach of contract is limited to injunctive relief and recovery of only economic losses resulting from the breach, while a plaintiff suing under a tort theory may recover for personal injury

resulting from the breach, including mental distress or other related injuries resulting from the wrongful disclosure of his or her confidential medical information.[15]

While the implied covenant of confidentiality traditionally has been applied in cases between doctors and patients, two pending cases are challenging the notion that other health care providers, such as pharmacists, do not owe the same level of care in maintaining the confidentiality of health information as do doctors, dentists or nurses.

In *Anonymous v. CVS*,[16] plaintiffs claim that their pharmacy breached its fiduciary responsibility to maintain confidential medical records by selling its customer information to CVS after it decided to close down. In refusing to dismiss the cause of action, Justice Charles Edward Ramos reasoned that "a fiduciary duty may arise, even in a commercial transaction, where one party reposed trust and confidence in another who exercises discretionary functions for the party's benefit or possesses superior expertise on which the party relied."[17]

In a similar suit against CVS and various pharmaceutical companies in Massachusetts,[18] class certification was affirmed for plaintiffs suing for the improper disclosure by CVS of its customers' personal information to a marketing company. The disclosures were allegedly made as part of a scheme to target individuals with relevant medical conditions for direct marketing by CVS on behalf of the pharmaceutical companies. While these cases regarding pharmacist and pharmaceutical liability have not been ultimately decided, it seems evident that medical confidentiality will no longer remain confined within the borders of the doctor-patient relationship.

Indeed, a bill currently pending before the New York Legislature may create a private cause of action against any health care provider who discloses patient health information without authorization. The proposed Personal Privacy Act of 2002,[19] if passed, would amend the public health law to create a statutory duty to maintain the confidentiality of health information. The proposed law would apply to all disclosures of health information subject to the public health law or "to which any other provision of law applies."[20] If the act is passed, it will take effect Jan. 1, 2002, more than a year earlier than the deadline for compliance with the HIPAA privacy regulations.

Compliance Plan

The best course of action for a covered entity wishing to avoid liability for the failure to comply with HIPAA is to develop and implement a comprehensive HIPAA compliance plan. The size, complexity and sophistication of the covered entity will dictate the level of the plan's complexity.

The regulations require that a privacy officer be appointed. A HIPAA compliance team should be identified as well. The team should represent all affected aspects of the organization. Team work is critical to the development of functional policies that are both compliant and relevant to the organization's current function and culture.

The first task of the HIPAA team is to perform or supervise the performance of a risk analysis. The analysis should include a map of the flow of PHI throughout the organization, including amount, type, direction, location of storage and risk of loss, and level of staff receiving information. It should also include identification of current business associates and categories of future associates and what information they receive and why. Once the analysis is complete, appropriate policies and guidelines to ensure compliance with all HIPAA privacy regulations should be developed and implemented. Ongoing training, supervision and documentation complete the compliance process.

The HIPAA regulations have far-reaching effects for every part of the health care community that has access to patients' PHI. By establishing regulations for the collection, storage and transmission of confidential data, HIPAA, in effect, sets the standard of care expected in the field. Failure to develop a functional compliance program will provide patients with additional ammunition in court and open the provider up to administrative, civil and criminal penalties.

•••••••••••••●●•••••••••••••

(1) Health Insurance Portability & Accountability Act of 1996, Pub. L No. 104-191 (codified in scattered sections of 42 U.S.C. and 18 U.S.C.).

(2) Health Insurance Portability & Accountability Act of 1996, Privacy Regulations, 45 C.F.R. §§160-164 (2000).

(3) The act is silent regarding the use of HIPAA in private actions. In the commentary to the act, however, the rights of third-party beneficiaries were discussed in the following manner:

> We do not intend this change to affect existing law regarding when individuals may be third-party beneficiaries of contracts. If existing law allows individuals to claim third-party beneficiary rights, or prohibits them from doing so, we do not intend to affect those rules. Rather, we intend to leave this matter to such other law. 45 C.F.R. §164.504(e) (2000).

(4) See *Costanza v. Seinfeld*, 693 NYS2d 897, 899 (Sup. Ct. New York County 1999) (noting that New York does not and has never allowed a common law claim based on privacy).

(5) See e.g., *Wedlock v. Troncoso*, 712 NYS2d 328, 332 (2000); see also *Chen v. United States*, 854 F2d 622, 627 (2d. Cir. 1988) (noting that the violation of a rule of an administrative agency does not constitute negligence per se, as it lacks "the force and effect" of a statute).

(6) See *George v. The Celotex Corp.*, 914 F.2d 26, 28 (2d. Cir. 1990).

(7) 45 C.F.R. §164.530(i)(1) (2000).

(8) 45 C.F.R. §160.203 (2000).

(9) 45 C.F.R. §160.202 (2000).

(10) 45 C.F.R. §164.524 (2000).

(11) See *Doe v. Community Health Plan-Kaiser Corp.*, 709 NYS2d 215, 217 (2000); *Tighe v. Ginsberg*, 540 NYS2d 99, 100 (1989); *Anderson v. Strong Memorial Hospital*, 531 NYS2d 735, 739 (1988).

(12) *Doe v. Roe*, 599 NYS2d 350, 357-58 (1993) (plaintiff permitted to proceed against physician for breach of oral contract to keep plaintiff's HIV status confidential).

(13) *Doe v. Roe*, 400 NYS2d 668, 674 (1977).

(14) See, e.g., *Doe v. Community Health Plan-Kaiser Corp.*, 709 NYS2d 215, 217 (2000); *Tighe v. Ginsberg*, 540 NYS2d 99, 100 (1989); *Anderson v. Strong Memorial Hospital*, 531 NYS2d 735, 739 (1988).

(15) See *MacDonald v. Clinger*, 446 NYS2d 801, 804 (1982).

(16) *Anonymous v. CVS*, 604804/99, *New York Law Journal*, March 9, 2001, at 19.

(17) Id. at 20.

(18) *Weld v. Glaxo Wellcome Inc.*, SJC-08363, class certified 5/1/01.

(19) Personal Privacy Act of 2002, Sen. 2330, Ass. 4230, Reg. Sess. (N.Y. 2001-2002). As currently written, different provisions of the bill are of greater or of lesser stringency than HIPAA; as such, it will remain to be seen how the Act will be interpreted and enforced in relation to HIPAA.

(20) Id at §1001.