HIPAA Privacy One Year Out:
Developments and Lessons Learned

WIGGIN AND DANA

Counsellors at Law

I. Introduction

A little more than a year ago, many of us were frantically copying Privacy Notices, completing HIPAA training and tweaking our privacy policies. While some commentators predicted mass chaos after April 14, 2003 as a result of the HIPAA privacy requirements, the intervening year has been manageable, thanks to the diligent efforts of the health care community in preparing for compliance. HIPAA is not just a test that a covered entity passed or failed on April 14, 2003, however; compliance is an ongoing process. This Advisory summarizes some of the past year's important HIPAA developments, and reminds providers about compliance deadlines that are now upon us.

II. Complaints and Enforcement

As of April 14, 2004, the Department of Health and Human Services Office for Civil Rights (OCR) had received more than 5,000 complaints from individuals regarding alleged HIPAA privacy violations. The largest number of privacy complaints have been lodged against private practices, followed by hospitals, pharmacies and health plans. OCR has already closed forty-eight percent of these complaints, including many that were dispatched easily on jurisdictional grounds (complaints regarding pre-compliance date behavior, complaints against non-covered entities such as employers, or complaints filed more than 180 days after the incident). The complaints that OCR decided warrant a further investigation fall into three broad categories:

- Lack of adequate safeguards (leaving charts in public areas, computer screens exposed to patients, etc.)
- Improper accessing of PHI (such as employees accessing PHI for non-treatment related reasons)
- Impermissible disclosure of PHI (to third parties not involved in treatment)

Interestingly, OCR has also received a large number of complaints regarding failures to disclose PHI to family members. While this is not a violation of HIPAA, OCR has provided technical assistance to providers that are the subject of these complaints, informing them that HIPAA permits such disclosures in many circumstances. Questions of disclosures to family members have received a lot of media attention since the HIPAA Privacy compliance date, and many providers that initially adopted very strict policies may be relaxing their approach due to the backlash. While providers may wish to be flexible in adapting their policies based on customer and patient feedback, remember that improper disclosures to family members can have serious implications.

To date OCR has not sought civil monetary penalties or other official sanctions for any cases it has investigated. One OCR representative said this was due to the cooperative way that providers responded to investigations, readily strengthening their policies or implementing training efforts in response to complaints. According to the director of OCR, fifty complaints have been referred to the Department of Justice, the agency

charged with investigating and enforcing criminal violations of the HIPAA rules. OCR representatives also indicated that there are no plans to institute audits, compliance reviews or other efforts to affirmatively seek out violations (rather than simply responding to complaints).

III. HIPAA in the Courts

Few cases have addressed the HIPAA Privacy Rule, given its newness, but some courts have considered the Privacy Rule's preemption provisions in connection with several discovery requests and subpoenas. The varying analyses and interpretations of these courts suggest that HIPAA preemption will be a knotty tangle for courts to parse in years to come. Here are some of the relevant decisions:

• A federal court in Louisiana concluded that HIPAA was more protective of patient privacy than State law, even though State law allowed patient records to be disclosed only with patient consent or based on a court order entered after a hearing. In an extremely technical and narrow reading, the court concluded that because Louisiana law (which related to disclosure of nonparty medical information during a proceeding) did not address "the form, substance, or the need for express legal permission from an individual," the State law was not "more stringent." Accordingly, the HIPAA provision that permits the disclosure of PHI as long as the parties have sought a qualified protective order preempted the Louisiana law. *United States ex rel. Stewart v. Louisiana Clinic*, 2002 WL 31819130 (E.D. La. 2002).

• A federal court in Maryland also concluded that HIPAA preempted Maryland law. A Maryland statute requires health care providers to disclose to defense legal counsel medical records relating to a patient's health, health care or treatment that forms the basis of a civil action instituted by a patient, without the patient's authorization. After the plaintiff in a medical malpractice action provided her medical records to the defense as part of discovery, the defendant's attorney sought to have discussions with her current treating physician without her notice or consent. The plaintiff objected to this attempt based on HIPAA, and the defendant argued that HIPAA was preempted because the Maryland statute was "more stringent" - according to the defendant, the Maryland law was mandatory and so was stronger than HIPAA. The court (correctly, in our view) rejected this argument and concluded that "more stringent" meant only state laws that were more protective or gave patients greater control over their records. *Law v. Zuckerman*, 2004 WL 438327 (D. Md. 2004).

• A state court in New Jersey concluded that HIPAA did not preempt a practice authorized by State supreme court precedent in which defendants in all personal injury cases are permitted to conduct informal interviews with plaintiffs' treating physicians, as long as specific patient authorization requirements are met. The court determined that these interviews did not conflict with the general principles of HIPAA, and as HIPAA does not expressly address informal discovery, the practice should be governed by New Jersey law.

The court did require, however, that the authorization forms used be revised to meet the HIPAA requirements. *In re PPA Litigation*, 2003 WL 22203834 (N.J. Super. L. Sept. 23, 2003).

• Two separate courts addressing the constitutionality of the Partial-Birth Abortion Ban Act of 2003 have also had to wrestle with HIPAA preemption. During discovery in these cases, Attorney General John Ashcroft issued subpoenas to several hospitals in New York and Illinois, seeking medical records of women on whom the plaintiff physicians performed certain abortion procedures. The court issued a protective order requiring redaction of certain identifiable information, and in both cases the plaintiff-doctors argued that "more stringent" state laws precluded the disclosure. In the New York case, the court concluded that the New York state law did not apply to federal cases, while the Illinois court concluded that the Illinois state law did because it was "more stringent." *National Abortion Fed'n v. Ashcroft*, 2004 U.S. Dist. LEXIS 4530, No. 03 C 8695 (S.D.N.Y. Mar. 18, 2004), *Nat'l Abortion Fed'n v. Ashcroft*, 2004 U.S. Dist. LEXIS 1701, No. 04 C 55, 2004 WL 292079 (N.D. Ill. Feb. 4, 2004).

The Seventh Circuit has affirmed the decision in the Illinois case, and the Second Circuit (which is responsible for a federal appellate region that includes Connecticut) has stayed the New York court's order pending its decision. Now that the government has withdrawn its subpoena for the New York hospital records, it is unlikely that the court will rule on the legal questions, but the variety of issues argued and analyses used demonstrate that neither attorneys nor courts quite have a handle on how to approach HIPAA preemption.

IV. Upcoming Deadlines

While many of us breathed a sigh of relief on April 14, 2003, the extended deadlines for some compliance tasks have now arrived. Remember the following:

• Covered entities were required to execute business associate agreements with vendors by April 14, 2004. When the final rule was issued in August of 2002, HHS gave covered entities an additional year beyond the original compliance date to sign these agreements with vendors that were under existing contracts, as long as certain requirements were met. The extended deadline has arrived, and providers should review their contracting process to be sure all existing vendor agreements are reviewed and BA language added where appropriate.

• Small health plans (defined as those plans that spend less than $5 million on premiums or health care costs) had an additional year to comply with the Privacy Rule. Many of these smaller plans are fully insured and have significantly fewer compliance obligations. Organizations that sponsor benefit programs for their employees still should review the nature of these benefits, however, and be sure they are aware of what their compliance obligations are. Common programs such as flexible spending accounts that reimburse

WIGGIN AND DANA

Counsellors at Law

medical expenses or employee assistance programs may be considered HIPAA-covered entities, and even smaller self-insured plans (for example, dental only) require compliance steps. A member of the HIPAA Practice Group (right) can assist you with questions about the scope of your HIPAA obligations.

V. Beyond Privacy to Security

The HIPAA Security Rule compliance date is April 21, 2005, the next major horizon. HIPAA security implementation needs to be structured and documented according to the Security Rule's standards and implementation specifications. Although specific IT solutions will help in achieving many of the security standards, there also are organizational, systemic and documentation issues that must be addressed. Make the time in advance to assess the Security Rule's requirements and design your implementation plan accordingly.

Nothing in this Client Advisory constitutes legal advice, which can only be obtained as a result of personal consultation with an attorney. The information published here is believed to be accurate at the time of publication, but is subject to change and does not purport to be a complete statement of all relevant issues.

HIPAA Practice Group

Jeanette C. Schreiber, Chair
203.498.4334/jschreiber@wiggin.com

Michelle Wilcox DeBarge
860.297.3702/mdebarge@wiggin.com

Maureen Weaver
203.498.4384/ mweaver@wiggin.com

Jennifer N. Willcox
203.498.4396/jwillcox@wiggin.com

One Century Tower
P.O. Box 1832
New Haven CT
06508-1832
Telephone 203.498.4400
Telefax 203.782.2889

400 Atlantic Street
P.O. Box 110325
Stamford CT
06911-0325
Telephone 203.363.7600
Telefax 203.363.7676

450 Lexington Avenue
Suite 3800
New York NY
10017-3913
Telephone 212.490.1700
Telefax 212.490.0536

One CityPlace
185 Asylum Street
Hartford CT
06103-3402
Telephone 860.297.3700
Telefax 860.525.9380

Quaker Park
1001 Hector Street, Ste. 240
Conshohocken PA
19428-2395
Telephone 610.834.2400
Telefax 610.834.3055

www.wiggin.com