THE HIPAA COLLOQUIUM
AT
HARVARD UNIVERSITY

HIPAA Litigation Risk Management: Essential Security Stop-Gaps for Privacy Implementation

Richard D. Marks
Davis Wright Tremaine LLP
1500 K Street, N.W., Suite 450
Washington, D.C. 20005-1272
(202) 508-6611

richardmarks@dwt.com

August 21, 2002
WASHINGTON, DC

The time is drawing near when the privacy, security, and transaction requirements of HIPAA will take hold. (HIPAA is the Health Insurance Portability and Accountability Act of 1996, Oublic Law 104-91, enacted August 21, 1996, codified at 42 U.S.C. §1320d.) As a practical matter, HIPAA's "covered entities" – hospitals, physicians and other providers who bill electronically; health plans; and health care clearinghouses – will be scrambling to meet two deadlines: August 14, 2003, the deadline for privacy rule implementation, and October 16, 2003, the date mandated for use of HIPAA's standard health care transactions in a nation-wide system of electronic data interchange (EDI).

This paper focuses on HIPAA's security requirements as they apply to covered entities, because security is the framework within which all HIPAA's privacy and transaction requirements are implemented. Simply, if covered entities cannot, in the statute's words, "ensure" security, then privacy measures are a hollow gesture, and HIPAA transactions are vulnerable to a world of mischief.

HIPAA – In Effect Today

The focus on final rules for transaction sets, privacy, and security, and the Department of Health and Human Services' inexplicable delays attending publication of the final rules for privacy and security, draw attention away from the parts of HIPAA that are in effect today. People continue to concentrate on those rules that are available in final form (even if the "final" rules are subjects of open rule makings aimed at new modifications), and ignore the underlying statute. Therefore, a brief review of HIPAA's present impact is in order.

HIPAA's standard for security is found at 42 U.S.C. § 1320d-2(d)(2):

Safeguards

Each [covered entity] who maintains or transmits health information shall maintain reasonable and appropriate administrative, technical, and physical safeguards –

- (A) to ensure the integrity and confidentiality of the information;
- (B) to protect against any reasonably anticipated –
  - (i) threats or hazards to the security or integrity of the information; and
  - (ii) unauthorized uses or disclosures of the information; and
- (C) otherwise to ensure compliance with this part by the officers and employees of such person.

Under § 1320d-6, there are criminal sanctions for "[a] person who knowingly and in violation of this part . . . obtains individually identifiable health information relating to an individual; or discloses individually identifiable health information to another person . . . ." Note that the statute uses (and defines, in § 1320d(6)) the term, "individually identifiable health information." The proposed final privacy rule uses the term, "protected health information," but the statute does not depend on that definition and neither does the availability of criminal sanctions.

What then does it take to act "knowingly and in violation of this part . . . ."? The "knowingly" requirement in federal criminal law probably will be interpreted by courts to mean simply that a defendant knew he was making some use or disclosure of information. The

government probably will not need to prove that the person knew that he was doing something wrong in making the use or disclosure. This is a low threshold.

The more difficult question is whether acting "in violation of this part" requires violating the privacy or security rules. (The privacy rules have issued in final form, but will not be enforced earlier than April 2003. *Standards for Privacy of Individually Identifiable Health Information; Final Rule*, 65 Fed. Reg. 82462, 82463-71 (2000), to be codified at 445 C.F.R. pts. 160, 164. The security rules are available only in proposed form, having been published in August, 1998. *Security and Electronic Signature Standards; Proposed Rule*, 63 Fed. Reg. 43241 (1998) (to be codified at 45 C.F.R. pt.142) (proposed Aug. 12, 1998)) The answer probably is no. The reason is that § 1320d-2 (d)(2) requires each covered entity (a health plan, health care clearinghouse, or health care provider) to maintain reasonable and appropriate administrative, and physical safeguards . . . to ensure the integrity and confidentiality of the information [and] to protect against any reasonably anticipated . . .threats or hazards to the security of integrity of the information [and] unauthorized uses or disclosures of the information; and . . . otherwise to ensure compliance with this part by the officers and employees of such person."

What does all that mean? That there is *already in force* a hefty security requirement. It applies to covered entities that use or transmit individually identifiable health information."

For a hospital, physician practice, health plan, or clearinghouse, this existing statutory requirement should be motivation to focus on maintaining a high level of technical security and the business policies and actual practices that go with it. Somewhere, somebody will be the victim of a hacker attack (such as the attack against the University of Washington) or an internal mistake (such as at the University of Michigan) or wrongful conduct by a disgruntled or malevolent employee. Patient data will become public, possibly by posting to the web. A U.S. Attorney will conclude that this demonstrates such disregard for HIPAA's requirements that a criminal prosecution is warranted.

This is hypothetical at the moment, but not really speculative. Security in health care is not yet generally at the level that the statute specifies.

So, in asking what to do now, hospitals, physician practices, health plans, and clearinghouses should not slow their efforts in the area of security, even though Secretary Thompson is accepting a new round of comments on the final privacy rule and has yet to release the final security rule. Neither rule cuts off the current security requirements of the statute.

There is another, possibly more important, reason why covered entities' efforts to achieve a high level of security are important: the possibility of private suits under state law. Potential plaintiffs are patients (or classes of patients) whose medical information is disclosed due to a security breach. These plaintiffs can now point to the security obligations specified in § 1320d-2 (d)(2), quoted above. Experts will testify that this statutory standard requires covered entities to exercise a high level of care where security of individually identifiable health information is at stake. Most covered entities lack the necessary security; yet all are on notice that a high level has been required, and they have been since 1996. No wonder the plaintiffs' bar is keenly anticipating the opportunities that HIPAA presents.

Note also that the final privacy rule will go into effect on April 14, 2003. Subsection

164.530 (c) of the privacy rule, as proposed for amendment (*see Standards for Privacy of Individually Identifiable Health Information; Proposed Rule; Modification* 64 Fed. Reg. 1476 (March 27, 2002)), states:

> (c) (1) *Standard: Safeguards.* A covered entity must have in place appropriate administrative, technical , and physical safeguards to protect the privacy of protected health information.
>
> (2) *Implementation specification: Safeguards.* (i) A covered entity must reasonably safeguard protected health information from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements of this subpart.
>
> (ii) A covered entity must reasonably safeguard protected health information to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure.

This parallels § 1320d-2 (d)(2) of the statute. It also creates a mini security rule as part of the privacy rule. Of course, the proposed security is long and detailed, but this mini security rule will remain in place even after the final security rule is published and takes effect; and, meanwhile, as of April 14, 2003, it will offer an independent basis for a plaintiff (or class of plaintiffs) to file suit in the event that protected health information is disclosed due to a security breach.

Furthermore, if, as appears likely, the security rule is published in final form before April 14, 2003, it will become the *de facto* standard for interpreting the appropriateness of security measures that a covered entity adopts under subsection 164.530 (c) of the privacy rule. Thus months before the final security rule comes into force in its own right, it will, as of the date it is published, essentially be incorporated wholesale into the privacy rule by virtue of subsection 164.530 (c).

Furthermore, although HHS may not enforce the final privacy rule until 2003, that would not prevent a private plaintiff from using subsection 164.530 (c) as one basis for a suit on negligence or similar grounds under state tort law.

Consequently, covered entities – particularly hospitals and physician practices – should initiate security upgrade projects as fast as practicable. This involves protecting legacy systems (*all systems* that carry individually identifiable health information); analyzing and redesigning clinical and administrative information flows; and learning about options for better security in access, storage, and transmission of these data. There is a great deal to do. Even if HIPAA's compliance deadlines are increased from two years to four (just a hypothetical example – there is no guarantee of this or any similar postponement), there is still great urgency in getting started now in order to finish on time, and with due regard for budgets.

Stop-Gap Security Planning for the April 14, 2003 Deadline

Many covered entities, particularly among the provider community, have hesitated to

begin implementing a full-scale HIPAA security program because HHS has not yet published the security rule in final form. Thus, they have set themselves up for a cruel irony, based on the interplay of the HIPAA statute (§1320d-2(d)(2)), subsection 164.530 (c) of the privacy rules, and the final security rules *as they may appear any time in the next one-to-four months*. In essence, on April 14, 2003, these covered entities will be faced with substantial civil litigation exposure (plus potential criminal liability) if the security measures that are required under subsection 164.530 (c) of the *privacy rules* do not measure up to whatever is in the final security rule, as read in light of that statute's command to *ensure* the integrity, confidentiality, and security of protected health information.

Further, as of April 14, 2003, officers and directors potentially face personal civil and criminal liability if their organizations have not implemented HIPAA security measures in a way that satisfies the standards of the business judgment rule and of Chapter 8 of the federal Criminal Sentencing Guidelines. The business judgment rule is applied in many states, though Delaware law is usually the starting point for understanding the doctrine and its development. *See In re Caremark International Derivative Litigation*, 698 A.2d 959 (Del Ch. 1996) (even though directors and officers may not be liable for wrongdoing that they have no reason to suspect, they have an affirmative duty to establish a compliance system); *see also Kahn v. MSB Bancorp., Inc.*, 24 Del. J. Corp. L. 266, 1998 WL 409355 (Del. Ch.) (protection under the business judgment rule may be lost through gross negligence); *In re Baxter International, Inc. Shareholders Litigation*, 654 A.2d 1268 (Del. Ch. 1995) (permissible under Delaware Code for corporation to exempt directors from personal liability, and plaintiff must then show bad faith, intentional misconduct, or knowing violation of law); *Smith v. VanGorkom*, 488 A.2d 858 (Del. 1985) (board decision must be "informed"); *Graham v. Allis-Chalmers Mfg. Co.*, 188 A.2d 1269 (Del. 1963) (directors have no duty affirmatively to seek out corporate employees' wrongdoing). To gauge the applicability of the business judgment rule in New York, and in a health care context, *see In re Oxford Health Plans, Inc., Securities Litigation*, 192 F.R.D. 111 (U.S.D.C. S.D.N.Y. 2000). For the applicability of the business judgment rule to non-profits (a significant proportion of health care entities), *see, e.g., Scheuer Family foundation, Inc. v. 61 Associates*, 179 A.D.2d 65, 582 N.Y.S.2d 662 (App. Div. 1st Dept. 1992).

Health care "covered entities" face substantial, practical time and budget limitations in implementing sufficient security measures by April 14, 2003, in order to satisfy the federal duty of care. Note that, by virtue of HIPAA's preemption rules, it is this federal duty of care that will become the standard for measuring tort claims in lawsuits under *state* law – for example, suits by patients whose protected health information has become public through the work of hackers, or through carelessness of a hospital or members of its workforce.

Here is a list of seven common-sense steps to accelerate HIPAA security planning and implementation:

1. Bring top management and the board of directors actively into oversight of the enterprise's HIPAA project, and make sure they remain informed about the progress of the project through periodic, detailed reports from the project team.

2. Designate a Security Officer and a Privacy Officer (two different posts – neither should be in the General Counsel's office).

3. Budget iteratively, as understanding grows of the new obligations imposed by HIPAA.

4. Understanding and implementing encryption technology is basic to HIPAA. Contact vendors of security technology to learn about the options available in the market. However, plan to implement most of the new technology *after* April 14, 2003. There simply is insufficient time to do more than plan for most of this new technology before the April deadline. Moreover, there are likely to be substantial financial constraints that inhibit a rapid selection and deployment of enterprise security technology.

5. Contact legacy system vendors and ask for details about HIPAA system deployment *and* warranties. (Meanwhile, *every* new contract for hardware, software, data communications, and related services should contain a HIPAA covenant. It should state that the vendor will negotiate with you in good faith, after the final HIPAA security and privacy rules are published, to amend sales, license, or maintenance agreements in order to allow you to comply with HIPAA. Further, there should be a clause that allows you to terminate the agreement if a satisfactory amendment for HIPAA compliance cannot be negotiated.)

6. Legal standards drive the technological and business process choices, so educate counsel and involved them in the HIPAA planning and implementation process.

7. Maintain a litigation perspective; think about privilege. It will help the enterprise your colleagues, who will feel the ultimate impact of HIPAA.

Meeting HIPAA's challenges is not just an information technology project, and it also is not just a compliance project. Rather, the budgetary, cultural, business process, and technological changes that HIPAA demands will make this an all-enterprise effort. To succeed, it must be supported from the top.