

MONDAY, NOVEMBER 6, 2000

Patient Health Data Goes On-Line

Healthcare Industry Must Prepare to Comply With Proposed Federal Privacy Rule

**BY JACKIE HUCHENSKI
AND LINDA ABDEL-MALEK**

WIDESPREAD ACCESS to patients' medical information through the Internet is right around the corner. Right now, there are numerous Web sites being developed to connect health care providers, health plans and others in the health care community and to gain access to an individual's medical information as necessary.

This proliferation of e-health Web sites as well as the general movement toward storing and transmitting health care information on computers is due, in large part, to the cost-cutting benefits that these media present to the healthcare industry. Administrative costs associated with the health care industry are unusually high compared to other industries, and this provides a large incentive to utilize electronic means of maintaining and transmitting health care information.

Setting up high-speed connections among providers, patients and health insurers, laboratories, nursing homes, pharmacies and others in the industry to pay bills, access and transfer medical records information, obtain immediate tests results, grant referrals, enroll in a health plan, provide treatment, issue prescriptions and schedule appointments via computer is the future of health care.

A patchwork of state and federal laws currently governs the confidentiality of some of this information. However, the federal government is about to extend such protections in a major and unprecedented manner. In a move that has swept the health care industry with controversy,

the government has recently indicated its intent to regulate such information by introducing a series of five administrative simplification rules governing the privacy and security of electronic medical records,¹ and the standards used for electronic data interchange of such information.

On Aug. 17, 2000, the first of these rules was published in final form, called "Transactions and Code Sets," which establish standard data content and formats for submitting electronic claims and other administrative health transactions. In this article, we focus on the HIPAA (Health Insurance Portability and Accountability Act) Privacy Rule, as it is typically called and which, although not yet finalized at the time of this writing, is expected to be published in final form before the end of this year.

Privacy Rule Generally

In November 1999, the Secretary of Health and Human Services proposed the HIPAA Privacy Rule in order to protect the privacy of an individual's health care information when transmitted or maintained electronically.² The Rule was proposed pursuant to authority granted to the Department of Health and Human Services by Congress in the Health Insurance Portability and Accountability Act of 1996.³

The potential and serious civil and criminal liability for failure to comply with the Privacy Rule, as well as the onerous administrative costs which the health care industry must absorb in order to comply with it, demand a close review of the Rule's implications. Although, as stated earlier, the Privacy Rule is still in proposed form, it is unlikely that many of the core concepts will be changed significantly. Below is an overview of its significant aspects.

The Privacy Rule generally protects the use and disclosure of a person's "protected

health information" (PHI). That term is defined as "individually identifiable health information" that is or has been electronically transmitted or maintained⁴ by a "Covered Entity" (health plans, health care clearinghouses and health care providers) including paper progeny of such electronic information.⁵

Covered entities generally have 24 months from the date the Privacy Rule becomes effective to bring their operations into compliance (the effective date begins 60 days after the final version is published in the Federal Register). Covered entities which are small health plans have 36 months from the effective date to comply.⁶

The Privacy Rule preempts state law with respect to the confidentiality of patient information except in the following three circumstances: (1) state laws that the Secretary of Health and Human Services (HHS) determines are necessary for certain purposes set forth in the statute; (2) state laws that the Secretary determines address controlled substances; and (3) state laws relating to the privacy of individually identifiable health information that are contrary to and *more stringent than* the federal requirements (emphasis added).⁷

As a practical matter, the majority of New York's laws in this area appear to be consistent with the Privacy Rule already. However, in some cases, current New York law may be deemed more stringent than the Privacy Rule — for example in the context of disclosing HIV-related information.⁸ Each applicable current and future New York law will have to be analyzed for preemption individually, and such analysis is beyond the scope of this article. Pursuant to the Rule, a state may submit a written request to the Secretary of HHS requesting that a certain provision of law be exempted from preemption pursuant to an advisory opinion issued by the Secretary.⁹

Jackie Huchenski, a partner with Moses & Singer LLP, is the chairwoman of the healthcare practice group and one of the co-chairs for the firm's e-health law practice. **Linda Abdel-Malek** is a senior associate in the healthcare group. **Glen Reitman**, an associate with the firm, assisted in the preparation of this article.

Business Partners

Although the Privacy Rule's authority extends directly to covered entities, its mandates with respect to disclosure of PHI from covered entities to their business partners regulate business partners indirectly. A "business partner" is defined in the rule as

a person to whom [a] covered entity discloses protected health information so that the person can carry out, assist with the performance of, or perform on behalf of, a function or activity for the covered entity. "Business partner" includes contractors or other persons who receive protected health information from the covered entity (or from another business partner of the covered entity) for the purposes described in the previous sentence, including lawyers, auditors, consultants, third-party administrators, health care clearinghouses, data processing firms, billing firms and other covered entities. "Business partner" excludes persons who are within the covered entity's work force.¹⁰

The business partner concept has proved to be quite controversial within the health care industry. HHS was not granted authority by Congress to oversee the activities of entities other than covered entities, and many in the industry view the creation of the "business partner" definition and the accompanying requirements that covered entities must place on their business partners as an end run around such lack of authority. Specifically, before disclosing PHI to a business partner, the covered entity must receive "satisfactory assurance" from such business partner that the information will be kept confidential.¹¹ The Privacy Rule defines "satisfactory assurance" as a contract between the covered entity and the business partner which must contain specific provisions outlined in the regulations.¹² The only instance in which such a contract is not mandated is when a covered entity that is a health care provider discloses PHI to another health care provider for purposes of consultation or referral.

Required contract provisions include, but are not limited to: (1) language which prohibits the use or disclosure of PHI by the business partner other than as stated in the contract; (2) language that requires

the business partner to incorporate appropriate safeguards to prevent use or disclosure of PHI in a manner that is not covered in the contract; (3) a requirement that the business partner ensure that any PHI disclosed by such business partner to subcontractors and agents be subject to the same restrictions covered in the contract between the business partner and the covered entity; (4) a provision that any persons who are the subjects of the PHI disclosed to the business partner are intended third-party beneficiaries to the contract (arguably providing an individual right to sue that is not permitted with respect to covered entities under the Rule); and (5) language that provides that if a business partner violates any of the terms of the contract, the Covered Entity may terminate the contract.¹³

The Privacy Rule does not require a covered entity to monitor its business partner's activities. It does, however, provide that a covered entity will be held liable for a business partner's violation of its contract if the covered entity knew or should have known of such violation and did not take reasonable steps to either cure the breach or terminate the contract.¹⁴

The Privacy Rule requires covered entities that are health plans and providers to develop a series of policies and procedures aimed at protecting individuals and allowing them certain rights with respect to their PHI [protected health information]

...

Use and Disclosure

In all situations other than the exceptions described herein, specific written consent is required prior to using or disclosing protected health information. Additionally, when any PHI is disclosed, the general rule is that only the minimum information necessary to comply with the need for such PHI should be disclosed. There are certain exceptions to this general rule requiring specific authoriza-

tion from the patient and disclosure of only the minimum information necessary, however. These exceptions fall into two general categories: "permissive disclosures" where individual consent is not required, and "mandatory disclosures" where individual consent is also not required.

Pursuant to the first category, PHI can be used without prior written consent if:

- it is necessary for treatment,¹⁵ payment¹⁶ or health care operations,¹⁷
- the information is de-identified — this essentially means that the information is anonymous, or that at minimum, no reasonable person could discern to whom the information is referring,¹⁸
- the information is given to a business partner for purposes of treatment, payment or health care operations, or
- the information is to be used solely for certain national purposes (public health activities, oversight of the health care system, judicial and administrative proceedings, law enforcement, directory information, research (with special requirements), and in emergencies).¹⁹

Pursuant to the second category, "mandatory disclosures," PHI *must* be disclosed, and does not require individual consent prior to disclosure, if:

- an individual requests to examine his or her own PHI, or
- the Secretary of HHS requires disclosure of PHI in connection with an investigation.²⁰

For uses and disclosures requiring individual consent, the Privacy Rule requires specific information to be provided prior to any such use or disclosure, and has provided a "model consent form" in the proposed regulations for this purpose. The model form specifies the elements that must be included in a consent form if the request for PHI is made by either (a) an individual for disclosure to third parties, or (b) a Covered Entity or other third party.²¹

Individual Rights

The Privacy Rule requires covered entities that are health plans and providers to develop a series of policies and procedures aimed at protecting individuals and allowing them certain rights with respect

to their PHI (clearinghouses are excluded from all but the requirements to keep records of disclosures and provide an accounting of such disclosures):

- notifying individuals of its information practices with enough specificity to give individuals adequate notice of expected uses and disclosures of PHI. The notice must include specific language set forth in the Rule and must be distributed by health plans at the following times:

- by the date that the health plan is required to be in compliance with the final Privacy Rule (i.e., the date that is either two or three years from the effective date of the final Rule, depending upon the size of the health plan),
- at enrollment,
- within 60 days of a material change to the practices, and
- every three years.²²
- The Privacy Rule places additional requirements on providers by requiring that they must provide such notification at the time of first service delivery within a year of the effective date of the Privacy Rule. Providers must also post the notice in a clear and prominent place for individuals to read as well as have copies available for individuals to take with them.²³

- granting individuals access to their PHI for the entire time that the Covered Entity maintains such information,²⁴

- keeping records of all disclosures of PHI and accounting to individuals for disclosures of their PHI, including disclosures authorized by the individual, and providing the date of each disclosure, the name and address of the person or organization to whom the disclosure was made and a description of the information released;²⁵ and

- granting individuals the right to amend and correct and apprising individuals of such right, including informing individuals when their amendments and corrections have been accepted and apprising relevant parties of such changes, including business partners, as well as notifying individuals when their amendments and corrections have not been accepted.²⁶

Compliance Program

A very significant component of the Privacy Rule is the requirement that a

compliance program be instituted by every covered entity that handles PHI. Structurally, these requirements are similar to those imposed on Medicare + Choice organizations²⁷ or health care entities operating under a "corporate integrity agreement" with the Office of Inspector General of HHS. However, the substance of such a compliance program is somewhat different than those currently in place.

Specifically, a covered entity must do the following:

- designate a Privacy Official responsible for developing and implementing the privacy policies and procedures of the covered entity;²⁸
- train all of its staff members who are in contact with PHI about use and disclosure of PHI by two years after the date on which the Privacy Rule is effective;²⁹
- implement sanctions for employees' violation of the covered entity's policies and procedures;³⁰
- establish and implement safeguards to protect the privacy of PHI;³¹
- establish and implement a complaint process, which would include designating a contact person to receive complaints and maintaining a record of all complaints received;³² and
- establish procedures for mitigating harm caused by unauthorized disclosures of PHI.

One important point to note is the

A very significant component of the Privacy Rule is the requirement that a compliance program be instituted by every covered entity that handles PHI.

duty of the covered entity to mitigate any harm caused by the use or disclosure of PHI in violation of the Rule. Under the Privacy Rule, this requirement could place significant burdens on the covered entity because the duty extends not only to the covered entity's own employees, but arguably, as discussed previously, to

the violations of its business partners as well.

Enforcement and Penalties

The Secretary of HHS is authorized to enforce the Privacy Rule through independent investigation and audit, as well as through investigations performed in response to individual complaints.

Individuals do not have a private right of action under the rule (although, as stated in the Business Partner section above, they are third-party beneficiaries of business partner contracts and thus arguably have a private right of action by virtue of such status). Individuals do, however, have the right to file a complaint with the Secretary if they believe that a covered entity has violated the Privacy Rule.³³ Such individuals may be subjects of PHI which has been improperly used or disclosed, or employees acting as whistleblowers. Any enforcement action undertaken by the secretary, whether independently or in response to a complaint, may result in the imposition of civil monetary penalties of up to \$25,000 per violation, per calendar year, and criminal penalties of up to \$250,000 and/or 10 years in prison.³⁴

.....●●●.....

(1) These include the following: Transactions and Code Sets (published in final form at 65 Fed. Reg. 50312); National Provider Identifier (introduced at 63 Fed. Reg. 25320); National Employer Identifier (introduced at 63 Fed. Reg. 32784); Security and Electronic Signature Standards (introduced at 63 Fed. Reg. 43242); and the Privacy Rule (introduced at 63 Fed. Reg. 59918).

(2) See 64 Fed. Reg. 59918. The Privacy Rule proposes to amend Title 45 of the C.F.R., Parts 160 through 164. Please note that all references to the CFR are to the proposed regulations.

(3) P.L. 104-191.

(4) For purposes of the definition of PHI, "(i) 'Electronically transmitted' includes information exchanged with a computer using electronic media, such as the movement of information from one location to another by magnetic or optical media, transmissions over the Internet, Extranet, leased lines, dial-up lines, private networks, telephone voice response and 'faxback' systems. (ii)

'Electronically maintained' means information stored by a computer or on any electronic medium from which information may be retrieved by a computer, such as electronic memory chips, magnetic tape, magnetic disk or compact disc optical media." The final rule may also extend to such health information in paper form. PHI excludes "(i) [i]ndividually identifiable health information in education records covered by the Family Educational Right and Privacy Act, as amended, and (ii) [i]ndividually identifiable health information of inmates of correctional facilities and detainees in detention facilities." 45 CFR §164.504.

(5) See 45 CFR §160.102.

(6) See 45 CFR §164.524. A "small health plan" is defined as a health plan with annual receipts of \$5 million or less, (see 45 CFR §160.103).

(7) 45 CFR §160.203.

(8) See Public Health Law §§2780 and 2782.

(9) The procedure for such advisory opinions is outlined in 45 CFR §160.204.

(10) 45 CFR §164.504.

(11) 45 CFR §164.506(e)(2).

(12) See 45 CFR §164.506(e).

(13) *Id.*

(14) *Id.*

(15) "Treatment" means the provision of health care by, or the coordination of health care (including health care management, and disease management) among, health care providers; the referral of a patient from one provider to another; or the coordination of health care or other services among health care providers and third parties authorized by the health plan or the individual. 45 CFR §164.504.

(16) "Payment" is defined as:

(1) The activities undertaken by or on behalf of a covered entity that is: (i) A health plan, or by a business partner on behalf of a health plan, to obtain premiums or to determine or fulfill its responsibility for coverage under the health plan and for provision of benefits under the health plan; or (ii) A health care provider or health plan, or a business partner on behalf of such provider or plan, to obtain reimbursement for the provision of health care.

(2) Activities that constitute payment include: (i) Determinations of coverage, improving methods of paying for coverage policies, adjudication or subrogation of health benefit claims; (ii) Risk adjusting amounts due based on enrollee health status and demographic characteristics; (iii) Billing, claims management, and medical data processing; (iv) Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges; and (v) Utilization review activities, including precertification and preauthorization of services. 45 CFR §164.504.

(17) "Health care operations" are activities by or on behalf of a health plan or health care provider to carry out its management functions necessary for the support of treatment or payment including but not limited to conducting quality assessment and improvement activities; reviewing competence or qualifications of health care professionals and evaluation of practitioner and provider performance; activities relating to insurance; insurance rating conducting and arranging for medical review and auditing services, including fraud and abuse detection and compliance programs; and compiling and analyzing information for legal

proceedings. 45 CFR §164.504.

(18) The Privacy Rule assigns 19 unique identifiers to information that render it "individually identifiable". These are as follows: (1) name; (2) address; (3) names of relatives; (4) name of employers; (5) birth date; (6) telephone numbers; (7) fax numbers; (8) electronic mail addresses; (9) social security number; (10) medical record number; (11) health plan beneficiary number; (12) account number; (13) certificate/license number; (14) any vehicle or other device serial number; (15) Web Universal Resource Locator (URL); (16) Internet Protocol (IP) address number; (17) finger or voice prints; (18) photographic images; and (19) any other unique identifying number, characteristic or code that the Covered Entity has reason to believe might be available to an anticipated recipient of the information. See 45 CFR §164.506. If these identifiers are stripped from the information at issue, such information is deemed under the Rule to be "de-identified".

(19) See generally 45 CFR §§164.506; 164.510.

(20) *Id.*

(21) See generally 45 CFR §164.508 and 64 Fed. Reg. 59918, 60065.

(22) 45 CFR §164.512.

(23) *Id.*

(24) 45 CFR §164.514.

(25) 45 CFR §164.515.

(26) 45 CFR §164.516.

(27) See, e.g. 42 CFR §422.501(b)(3)(vi).

(28) 45 CFR §164.518(a).

(29) 45 CFR §164.518(b).

(30) 45 CFR §164.518(e).

(31) 45 CFR §164.518(c).

(32) 45 CFR §164.518(d).

(33) 45 CFR §164.522(d).

(34) 45 CFR §§164.518(c), 164.522(b).

MOSES & SINGER LLP

Jackie Huchenski
jhuchenski@mosessinger.com

Linda Abdel-Malek
labdelmalek@mosessinger.com

1301 Avenue of the Americas
New York, NY 10019-6076
212.554.7800 Fax: 212.554.7700
www.mosessinger.com