VOLUME 6 • NO. 2 • FEBRUARY 2003

monthly memo
mvma ipa

Physicians Committed to Quality

An important announcement from Richard B.Toll, M.D., MVMA President

Contacting MVMA Staff

David Phelps, MD,
Medical Director
dphelps@mvphealthcare.com
388-2647

Deb Zadrozny, RN,
Director of Operations
dzadrozny@mvphealthcare.com
388-2690

Rebecca Klehn,
Professional Liaison
rklehn@mvphealthcare.com
388-2246

Paula Pecoraro, RN,
Professional Liaison
ppecoraro@mvphealthcare.com
388-2209

Gail Sapone, RN,
Professional Liaison
gsapone@mvphealthcare.com
388-2605

Sharlene Campbell,
Administrative Assistant
scampbell@mvphealthcare.com
388-2461

A Word on Patient Privacy

by Iseman Cunningham Riester & Hyde, LLP

Please note: This article is not intended to provide legal advice and does not create an attorney-client relationship with the reader.

Every physician has heard jokes about hospital gowns—the ones that open in the back—and probably first heard them long before he or she even dreamed of becoming a physician. In a allegorical sense, the jokes illustrate a common patient fear: the gown is the "health care system," and the opening is a built-in shortcoming that permits an embarrassing display of personal information to the world which occurs—quite literally—behind the patient's back.

No doubt patients look to physicians to safeguard their private information. Physicians, too, have long accepted this responsibility as a cornerstone of their practical philosophy. In the classical version of the Hippocratic oath, the practitioner swears:

> WHAT I MAY SEE OR HEAR IN THE COURSE OF THE TREATMENT OR EVEN OUTSIDE OF THE TREATMENT IN REGARD TO THE LIFE OF MEN, WHICH ON NO ACCOUNT ONE MUST SPREAD ABROAD, I WILL KEEP TO MYSELF, HOLDING SUCH THINGS SHAMEFUL TO BE SPOKEN ABOUT.

In 1964, Louis Lasagna, Dean of Academic Medicine at Tufts University, offered the following modern version:

> I WILL RESPECT THE PRIVACY OF MY PATIENTS, FOR THEIR PROBLEMS ARE NOT DISCLOSED TO ME THAT THE WORLD MAY KNOW.

In both versions the privacy of the patient is paramount.

In 1996, Congress enacted the Health Insurance Portability and Accountability Act of 1996, commonly referred to by its acronym "HIPAA," setting in motion a complex series of events that has culminated in three major sets of regulations impacting the entire health care industry. One fundamental purpose of HIPAA was to strengthen the protection of patient privacy—in effect, to close that embarrassing opening in the back of the hospital gown. Many continue to debate whether HIPAA meets that objective. But the regulations are enforceable regardless of whether physicians believe the new rules are useful or needed.

With the advent of HIPAA, a breach of patient privacy is no longer simply shameful—it can also be criminal. The most egregious HIPAA offense is selling a patient's personal health information for commercial gain, which carries a fine of up to $500,000 and/or imprisonment for ten years. Even minor violations can be expensive: $100 per violation to a maximum of $25,000 in one year.

HIPAA privacy regulations will go into effect on April 14, 2003. Rumors abound of extensions, continued revisions to the rule, even of retraction. These should be dismissed. The only "extension" for compliance with privacy regulations is a one year grace period for working "business associate" language into existing written contracts and the grace period only pertains under certain circumstances. For everything else under the privacy sun, April 14th is the deadline.

Other aspects of HIPAA have different implementation timeframes. A second major set of regulations, the "transactional" standards, went into effect in October of 2002. These are electronic data interchange standards that govern "standard transactions" such as health plan eligibility verification, claims processing or transmission of encounter data, and claims payment. Standard transactions must comply with the new standards if they are conducted electronically.

A third major set of regulations, the HIPAA "security" standards, were published in final form in late February. The security standards will also affect how physicians safeguard patient privacy, although to a lesser degree than the privacy standards.

continued

The stiff penalties for HIPAA privacy violations underscore the importance that Congress has given to patient privacy and portend a serious enforcement effort. The need for physicians to understand HIPAA also stems from the fundamental obligation that each physician has to protect patient privacy, even in the absence of federal standards and potential fines.

Getting Your Arms Around HIPAA

Understanding HIPAA is a daunting task. It is commonly known that the HIPAA privacy rules, when considered together with available commentary from CMS (the Centers for Medicare & Medicaid Services—formerly "HCFA") and informal "guidance" from CMS and the Office of Civil Rights (which administers the privacy rules), are longer than Leo Tolstoy's epic novel *"War and Peace."* Few have that kind of time, even considering HIPAA's importance to the industry and the risks of non-compliance.

To make matters worse, understanding the federal rules is only half of the analysis. HIPAA was designed to be a "floor," or a minimum standard regarding protection of patient privacy. Individual states may have laws that provide more protections and in such cases the state law will prevail. In New York, for example, laws governing disclosure of HIV- and AIDS-related information contain more stringent protections than HIPAA. Physicians must continue to apply the stricter New York standard.

In addition, many of the HIPAA privacy rules incorporate a "minimum necessary" standard, leaving the physician with the burden of determining whether certain information is, or is not, reasonably necessary to a transaction so as to justify disclosure.

To comply with HIPAA, physicians must, minimally:

- develop and implement compliant office policies and procedures relating to privacy—affecting everything from billing and reimbursement policies to patient sign-in and waiting room procedures;
- designate a privacy officer to be responsible for overseeing HIPAA compliance;
- revise existing relationships with payors, vendors and suppliers—(even including, under some circumstances, the office cleaning service); and
- conduct training as necessary for staff to carry out policies and procedures in compliance with the privacy standards.

Reducing these tasks to bullet points is not intended to belie the importance or difficulty of any one task. Neither is it intended to convey that HIPAA compliance may be neatly compartmentalized and digested. Quite the contrary: working through HIPAA issues is messy stuff.

Consider, for example, the issue of patient authorization. HIPAA permits disclosures of health information for treatment or payment purposes without the need for a specific consent or authorization. New York law, however, requires physicians to obtain the patient's consent before revealing health information (except where the law otherwise requires or permits disclosure). In the old days, this issue was soft-shoed. The post-HIPAA environment no longer permits the question to languish: How will the physician obtain the patient's consent to release this information when such consent is required?

A full HIPAA implementation will require that these issues, and dozens of others that are equally messy, be answered.

Covered Entities: Who's In, Who's Out

HIPAA works by requiring "covered entities" to meet certain standards in the use and disclosure of patient health information. If a physician meets the definition of a "covered entity," the physician must comply with the HIPAA standards.

A physician is a covered entity if the physician transmits health information electronically in connection with a "standard transaction." A "standard transaction" includes transmission of claims or encounter data, payment of claims, coordination of benefits, or referral certification and authorization.

A physician is also a covered entity if another person or company conducts a standard transaction electronically on a physician's behalf. A physician using a billing service that submits claims electronically is a "covered entity" because the billing service is conducting an electronic "standard transaction" (i.e. claims submission) on the physician's behalf.

Protected Health Information

HIPAA protects health information identifying an individual or from which an individual's identity can be inferred or extracted. The privacy standards control how covered entities use and disclose "protected health information" regardless of whether it is stored electronically or on paper and regardless of whether the protected health information is used in a standard transaction.

Protected health information includes any information that relates to the past, present, or future health or mental health of an individual, or that relates to the provision of health care services to the individual or payment for health care services. Protected health information does not include information that is maintained by a covered entity in its status as an employer. It also does not include information that has been "de-identified"— meaning enough information has been removed from the record so that it does not identify the individual and could not be used to identify the individual.

Uses and Disclosures

HIPAA prohibits *all* uses and disclosures of protected health information except as specifically permitted by the privacy rules. Although many sections of the rule are broadly permissive, the underlying concept is that health information is off limits for use or disclosure unless HIPAA specifically permits the use or disclosure.

The privacy rules permit use and disclosure of protected health information for the purpose of carrying out treatment, payment, or health care operations. Treatment includes referrals and consults. Payment includes claim submission and payment. Health care operations includes credentialing, quality assurance/quality improvement, and many other managerial functions (business planning and strategy, customer service, and auditing are some examples).

HIPAA permits a number of disclosures to occur without specific authorization from the patient. Other uses of disclosures not pertaining to treatment, payment, or health care operations may only be accomplished pursuant to a written authorization. The form of the authorization must meet the requirements outlined in the privacy rules.

A Nutshell Implementation Strategy

HIPAA is a bear, no doubt, but one that physicians cannot flee from. Dealing with HIPAA will require some time, some patience, and a great deal of perseverance.

Phase 1: Education Attend seminars, read books, read the regulation itself if you are the daring sort. Develop a sense of the important themes. Learn to discriminate between genuine requirements and uninformed or misguided hyperbole. Yes, you do need to examine all of your existing policies and procedures, revise many of them and write some new ones. No, you (probably) do not need to hire two new supervisory employees, make your exam rooms "soundproof" and cease sending patient information by facsimile.

Phase 2: Planning HIPAA implementation begins with a "gap" analysis—a comprehensive review of your current practices to see how they measure up to HIPAA's standards. From the gap analysis, develop a game plan for the next phase, development.

Phase 3: Development This is where the nuts and bolts are put in place. The best development model will mix input from management, staff, and independent expert advice.

Phase 4: Execution In this phase policies and procedure are put into practice. Depending on the size of the physician practice, some areas of compliance may have proceeded to execution while others are still in development.

Phase 5: Testing As new policies and procedures settle in, a targeted testing effort should take place to ensure the new processes are working appropriately.

One thing physicians should *not* do is wait until early April and then purchase a "HIPAA-in-a-box" product. Chances are slight that a generic model will be appropriate for New York physicians due to the interaction between HIPAA and New York law, which imposes higher standards in many areas.

The other thing physicians should *not* do is ignore HIPAA. Turning a blind eye to the new privacy requirements will ultimately leave the physician feeling like the patient in the proverbial pre-HIPAA hospital gown.

To assist MVMA physicians in understanding HIPAA, attorneys from Iseman Cunningham Riester & Hyde will present an overview and discussion of the HIPAA requirements at the MVMA annual meeting on March 19, 2003, at 6:30 pm.

Contact info: Carol A. Hyde, Esq., Iseman Cunningham Riester & Hyde LLP, 9 Thurlow Terrace, Albany, NY 12203 (518) 462-3000.

Physicians Committed to Quality