MINTZ LEVIN COHN FERRIS GLOVSKY AND POPEO PC

BOSTON
WASHINGTON
RESTON
NEW YORK
NEW HAVEN

www.mintz.com

If you would like further information on these or any health law issues, please contact one of our health law attorneys.

Thomas M. Antone, IV.....202 434 7351
Linda D. Bentley 617 348 1784
Susan W. Berson 202 661 8715/212 692 6750
Susan L. Burke 202 661 8707
Raymond D. Cotton 202 434 7322
Thomas S. Crane 617 348 1676/202 661 8787
Hope S. Foster.....202 661 8758
Marie C. Infante.....202 434 7489
Ellen L. Janos 617 348 1662
Peter M. Kazon 202 661 8739
Bradley L. Kelly.....202 434 7395
Alvin J. Lorman 202 434 7373
Carolyn J. McElroy 202 434 7408
M. Daria Niewenhous.....617 348 4865
Laura J. Oberbroeckling 202 434 7333
Charles A. Samuels 202 434 7311
Lisa Marie Sylvia 202 434 7469
Stephen M. Weiner 617 348 1757

Michael D. Bell.....202 434 7481
Theresa C. Carnegie 202 661 8710
Deborah A. Daccord 617 348 4716
Erin Lewis Darling 202 434 7478
Valerie E. Hurt 202 434 7488
Gail K. Julie 212 692 6740
Karen S. Lovitch 202 434 7324
Nell M. Ma'luf 617 348 4496
Carrie Nixon 202 434 7349
Staci B. Patterson 202 661 8764
Jennifer Gulbrandsen Ruggiero.....202 434 7463
Diana Puknys Schad 202 434 7328
Eric S. Tower.....202 434 7344
Francine Wachtmann 617 348 4477

Advisory

April 2002

HEALTH LAW

The HIPAA Privacy Regulation: The Never-Ending Story

Our story thus far: In an effort to ensure the privacy of patients' health information, in 1996 Congress passed the Health Insurance Portability and Accountability Act of 1996, now known to all as HIPAA. In the waning days of the Clinton Administration, the Department of Health and Human Services (HHS), issued a massive and far-reaching final regulation (Privacy Regulation), which would have instituted a variety of new and comprehensive requirements related to the privacy of health information. The compliance date of those requirements is April 2003. The incoming Bush Administration was widely expected to significantly modify the final Privacy Regulation. However, although it requested additional comments on the impact of the Privacy Regulation, the new administration left the rule in place, promising instead to propose additional changes in the future to reduce the burdens associated with the rule.

In the latest episode, HHS made good on that promise, issuing a proposed rule on March 27, 2002 (Proposed Rule), which would, if made final, make significant changes in a number of key areas. In the discussion below, we focus on the following five areas: (1) new requirements for consents; (2) revision of the authorization requirements; (3) changes to the marketing provisions; (4) new proposals related to medical research; and (5) changes to the business associate provisions. Although this Advisory focuses on five key issues, the Proposed Rule contains other significant changes to the Privacy Regulation. Comments on the Proposed Rule are due April 26. Although this is a relatively brief comment period for such a complex proposal, HHS said it was necessary because by statute, any changes to the regulation must be final by October 13, 2002, six months before the Privacy Regulation's compliance date.

New Consent Requirements

The Proposed Rule significantly reduces the burden on providers with respect to obtaining an individual's consent to use or disclose protected health information (PHI) for treatment, payment, or health care operations (TPO) purposes. Under the original Privacy Regulation, health care providers with a direct treatment relationship with the individual are required to obtain written consent from the individual before using or disclosing the individual's PHI for treatment, payment, or health care operations. In response to providers' concerns about the unintended consequences of this requirement, the Proposed Rule would eliminate the consent requirement for health care providers with a direct treatment relationship with the individual, but would allow all health care providers to obtain a consent if they so chose.

Not only would covered entities have the option of obtaining or not obtaining consent, if a covered entity decided to obtain consent, it would be permitted to design its consent form and process however it chose because the Proposed

Rule eliminates the current standards for consents. Providers would have discretion in creating the consent form and deciding when and how to obtain the consent from individuals. A consent, however, could still only apply to uses and disclosures that are otherwise permitted by the Privacy Regulation — *i.e.,* a consent would not permit a covered entity to use or disclose PHI for purposes which would otherwise require an authorization (*e.g.,* uses or disclosures for research purposes). Furthermore, it is important to remember that states may impose their own standards regarding consent, which will still apply even though the Proposed Rule eliminates the consent requirements.

No Consent for Information Sharing

The Proposed Rule also would allow covered entities more freedom to share PHI with other covered entities and non-covered health care providers. The current Privacy Regulation permits covered entities to disclose PHI for treatment purposes, and to use and disclose PHI for their own payment and health care operations activities. However, covered entities must obtain an authorization in order to disclose PHI for the payment or health care operations of another entity. For example, where an ambulance service needed a patient's PHI from the treating hospital in order to bill the patient's insurer for the transportation provided, the hospital would be required to obtain an authorization from the patient before disclosing this information to the ambulance service. By contrast, the Proposed Rule would permit a covered entity to disclose PHI for the *payment* activities of other covered entities and non-covered health care providers. For instance, a physician could share a patient's PHI with a durable medical equipment supplier so that the supplier could establish that the equipment was medically necessary in order to obtain payment from the Medicare program for providing the equipment to the patient.

The Proposed Rule also would allow covered entities to disclose PHI for certain *health care operations* of other covered entities so long as each entity has, or has had, a relationship with the individual. Where the relationship between the individual and the covered entity has ended, the covered entity would be permitted to disclose the PHI if it related to the past relationship. In particular, covered entities would be allowed to disclose PHI to another covered entity for:

- quality assessment and improvement activities;
- population-based activities relating to improving health or reducing health care costs;
- case management;
- conducting training programs;
- accreditation, certification, licensing or credentialing activities; and
- health care fraud and abuse detection and compliance programs.

By limiting the sharing of PHI in this way, the Proposed Rule aims to protect the individual's privacy while still allowing covered entities to engage in activities necessary for the provision of high-quality and effective health care.

New Acknowledgement Requirement

Although the Proposed Rule eliminates the consent requirement, it does create a mechanism to ensure that individuals still have the opportunity to discuss with providers how their PHI will be used and disclosed. In particular, the Proposed Rule requires covered health care providers with a direct treatment relationship with the individual to make a good faith effort to obtain a written acknowledgment of receipt of the provider's *Notice of Privacy Practices.* This written acknowledgement would be required at the time of first service delivery — the same time that the *Notice* must be provided. The Proposed Rule would impose no other requirements for obtaining an acknowledgement, other than the requirement that it be in writing.

One way for providers to obtain an acknowledgement would be to require individuals to sign the paper *Notice* they are provided. Providers might also consider having the individual sign a separate list or initial a cover or end sheet of the *Notice* that would then be retained by the provider. A provider would also still be allowed to provide its *Notice* electronically; however, the provider's computer system would have to be capable of capturing the individual's acknowledgement of receipt electronically. It is important to note that the Proposed Rule would require only a good faith effort to obtain an acknowledgement from the individual. If a provider was unsuccessful in obtaining an individual's acknowledgement, so long as the provider documented its good faith efforts to obtain the acknowledgement and the reason that it was unable to obtain the acknowledgement, the provider would be in compliance with this requirement.

Revision of Authorization Requirements

The Privacy Regulation requires covered entities to obtain an individual's authorization before using or disclosing PHI for any purpose that is not otherwise permitted or required under the Privacy Regulation. The Proposed Rule would streamline and simplify the requirements for authorizations. Most importantly, the Proposed Rule would consolidate the authorization requirements by requiring *all* authorizations to contain the following core elements:

- a description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion;

- the identification of the persons or class of persons authorized to make the use or disclosure of the PHI;
- the identification of the persons or class of persons to whom the covered entity is authorized to make the use or disclosure;
- a description of each purpose of the use or disclosure;
- an expiration date or event that relates to the individual or the purpose of the use or disclosure;
- the individual's signature and date; and
- if signed by a personal representative, a description of his or her authority to act for the individual.

The Proposed Rule would also require *all* authorizations to contain the following notifications:

- a statement that the individual may revoke the authorization in writing, and either a statement regarding the right to revoke, and instructions on how to exercise this right, or to the extent the information is included in the covered entity's *Notice*, a reference to the *Notice*;
- a statement that treatment, payment, enrollment, or eligibility for benefits may not be conditioned on obtaining the authorization if such conditioning is prohibited by the Privacy Regulation, or, if conditioning is permitted by the Privacy Regulation, a statement about the consequences of refusing to sign the authorization; and
- a statement about the potential for the PHI to be subject to redisclosure by the recipient.

These changes would ease the administrative burden on covered entities by allowing them to create a single authorization form that could be used in most situations.

In addition, no longer would all authorizations have to disclose whether a covered entity will receive remuneration as a result of obtaining an authorization; only authorizations for marketing activities would be required to include information about remuneration, if applicable. The Proposed Rule would also clarify that the minimum necessary standard does not apply to uses or disclosures made pursuant to an authorization for any purpose, and that disclosures made pursuant to a valid authorization do not have to be included in an accounting provided to the individual. The exclusion of uses and disclosures made pursuant to an authorization from the accounting requirement significantly reduces a covered entity's obligation to account for disclosures. In essence, covered entities will only be required to track and account for disclosures made for so-called national priority purposes (*e.g.,* disclosures required by law, for public health activities, to law enforcement, in judicial proceedings) because TPO disclosures were already exempt from the accounting requirement.

Changes to Marketing Requirements

The Proposed Rule significantly modifies the Privacy Regulation's requirements related to marketing, including when a covered entity must obtain an authorization before making a marketing communication. While the Proposed Rule appears more restrictive in certain ways, it also relaxes some requirements related to marketing; therefore, it is unclear what the reaction of providers and consumers is likely to be.

The Privacy Regulation defines the term "marketing" as a communication about a product or service, the purpose of which is to encourage recipients of the communication to purchase or use the product or service. Certain broad areas are specifically carved out of this definition, however, including:

- disclosures that describe the participants in a health care provider network;
- disclosures describing whether, and to what extent, a product or service is furnished by an entity or covered by a health plan;
- communications to a patient related to his or her treatment; and
- communications made to recommend alternative treatments, therapies, providers or settings of care.

However, these "carve outs" would not usually apply if the provider receives payment from a third party for making the communication. A separate provision of the Privacy Regulation lays out the specific requirements for "marketing." While an authorization is usually required for any marketing disclosures, certain marketing communications are exempt from this requirement, including those occurring in a face-to-face encounter, those involving products or services of "nominal value," and those related to "health-related products and services" of the covered entity or a third party, but only if certain additional requirements are met. Even then, individuals have to be given the ability to "opt out" of future marketing communications.

Not surprisingly, the Proposed Rule concludes that both industry groups and consumer groups found the marketing provisions "complicated and confusing." Questions were raised about whether certain types of communications constituted marketing at all, such as those related to disease management or prescription refill reminders. In addition, many of those commenting on the Privacy Regulation stated that they were dissatisfied with provisions that permitted consumers to "opt out" of future marketing communications, but did not permit them to avoid such communications in the first place, before the marketing — and the use of their health information — occurred.

Simplified Marketing Provisions

To alleviate these concerns, the Proposed Rule attempts to simplify the marketing rules and to eliminate the numerous fine distinctions in the Privacy Regulation.

First, the Proposed Rule makes minor changes in the definition of marketing to make clear that the entity's intent in making the communication is not determinative. Rather, any communication about a product or service that encourages the recipient to purchase or use a product or service constitutes marketing.

Second, the Proposed Rule would eliminate entirely the Privacy Regulation's special provision setting out standards and implementation specifications for marketing. This provision was deemed no longer necessary because the new proposal takes the position that if the communication meets the definition of the term "marketing," an authorization would be required. As a result, if a communication constitutes marketing, it will not usually be permissible to make it without a patient authorization and then simply give the patient an opportunity to "opt out" later.

The Proposed Rule does continue to carve out from the definition of marketing those communications describing who is participating in a health care network, whether a particular service is covered and to what extent, and those related to treatment of the individual (*e.g.,* a letter from an insurer noting that a particular prescription drug is covered by its formulary). The Proposal also clarifies that communications related to case management or case coordination for the individual who is the subject of the PHI also are excluded from the definition of marketing.

Unlike the Privacy Regulation, however, these communications are excluded from the definition of marketing regardless of whether they are made orally or in writing and regardless of whether or not the entity is receiving remuneration from a third party for making the communication. According to the Preamble discussion, concerns were raised that the Privacy Regulation would limit the ability of providers and patients to communicate freely about treatment because a marketing communication related to treatment for which an entity was paid by a third party would require the patient's prior authorization. The Proposed Rule states that HHS determined that a health care provider should always be permitted to send out a prescription refill reminder, for example, even if the provider was compensated by a third party for that activity, and regardless of whether or not it had received an authorization from the patient.

Authorizations for Marketing

While the Proposed Rule eliminates the previous provisions establishing standards for the use and disclosure of PHI for marketing, it does add new marketing provisions related to authorizations. The new provision explicitly requires an authorization for a use or disclosure of PHI for marketing purposes, as that term is defined in the regulations. The Preamble to the Proposed Rule is quite specific that entities continue to be prohibited from selling lists of patients or enrollees to third parties or from disclosing PHI to third parties for independent marketing activities without the express authorization of the individual. Two previously existing exceptions are kept in this new section — face-to-face communication between a covered entity and an individual still does not require an authorization nor does a communication in the form of a promotional gift of nominal value. All other forms of marketing, as that term is defined in the Proposed Rule, would require authorization. Furthermore, if the entity making the communication expects to receive direct or indirect remuneration from a third party, that fact must be stated in the authorization itself.

The new marketing provisions appear to eliminate some of the confusion that exists in the Privacy Regulation. In addition, the proposal attempts to address the concerns of many privacy advocates that the Privacy Regulation does not adequately protect individuals from the initial disclosure of their PHI for marketing purposes, but simply gives them the opportunity to avoid subsequent disclosures through the opt out provisions. The biggest change in the new rules, however, is that all relevant communications related to treatment are carved out of the definition of the term "marketing," regardless of whether or not the entity making the communication is paid by a third party. This is likely to trouble some consumers, who may feel it continues to offer inadequate protection from unwanted marketing activities.

New Proposals for Medical Research

Since research does not fall within the definition of treatment, payment or health care operations, the Privacy Regulation requires that no PHI be used or disclosed for research purposes unless an authorization has been obtained, except in limited circumstances such as where a waiver of the authorization requirement is obtained from an IRB or a Privacy Board, based on enumerated criteria. (A Privacy Board is a new entity created by the Privacy Regulation to assess the privacy issues created by disclosures in research, without the individual's authorization.) This requirement was not without controversy as the so-called federal Common Rule (which governs federally-funded research) and the Food and Drug Administration's (FDA) regulations already impose requirements on research that many believe make the Privacy Regulation at best duplicative of, and in some cases contradictory to, existing requirements.

Revised Waived Criteria

In an attempt to make the Privacy Regulation more consistent with the Common Rule, the Proposed Rule reduces the number of criteria that must be met in order for a waiver to be obtained. The only two criteria listed in the Privacy Regulation that would be retained, if the Proposed Rule is adopted, would be the following: (1) the use or disclosure of protected information must involve no more than a minimal risk to the privacy of the individual, and (2) it must be found that the research could not practicably be conducted without the waiver or alteration. The waiver criteria contained in the Privacy Regulation relating to

destruction of identifiers, protection of identifiers, and written assurance against redisclosure, would become elements to be considered as part of the first criteria, the degree of risk to the individual's privacy interests. The other criteria in the Privacy Regulation relating to privacy risks versus anticipated benefits would be eliminated. Further, the Proposed Rule requests comments on the possible modification of the data set that would be considered identifiers for research purposes in order to allow for personally identifiable information to be removed from research information while retaining some identifiers that are critical to research and still be considered de-identified. This proposal is an attempt to respond to concerns that if information is de-identified, in compliance with the Privacy Regulation, it will be useless for research because all the key variables will have been removed.

The Proposed Rule includes several general proposals with respect to authorizations, many of which are discussed above. With regard to research specifically, the Proposed Rule would eliminate the distinction between authorizations for research involving treatment (*i.e.,* clinical trials) and authorizations relating to research that does not involve treatment. In addition, an authorization would no longer need to be a stand-alone document, but could be combined with other research-related documents, such as the consent to participate in the study.

In the research context, the Proposed Rule provides that the expiration date requirement for authorizations could be met by the statement "end of research study" or similar language. Further, if the authorization is for a covered entity to use or disclose PHI for the creation or maintenance of a research database or repository, the statement "none" could be used. However, if subsequent research is conducted using data in the database, the authorization would, at the least, need to contain the statement "end of the research study" as the expiration date. The full implications of this change are yet to be clarified. All of these proposals, however, are intended to facilitate and encourage important research to move forward while at the same time continuing to offer protection to research participants.

Transition Rules

The Privacy Regulation also contains specific transition rules for research studies. The current rules are different depending on whether the research does or does not include treatment. In the case of research that includes treatment, so long as legal permission was obtained to use or disclose PHI, that permission would remain valid (whether it complied with the authorization requirements or not) for information that was created or received before or after the compliance date. However, for research that does not include treatment, the permission would only be valid for information obtained before the compliance date. The Proposed Rule would eliminate the distinction between types of research and would permit a covered entity to use or disclose PHI obtained for a specific research project, either before or after the compliance date, if the covered entity had obtained before the compliance date a legal permission or authorization for the specific study — regardless of whether such permission complied with the Common Rule or FDA requirements, or with the Privacy Regulation's authorization requirements. The permission would be applicable as long as it was obtained before the compliance date, even if the study did not begin until after the compliance date. In addition, research conducted pursuant to a waiver of informed consent in accordance with the Common Rule or FDA regulations also would be grandfathered under the Proposed Rule.

New Business Associate Provisions

The Privacy Regulation permits the disclosure of PHI by a covered entity to a business associate that performs specified functions on behalf of the covered entity, so long as the covered entity obtains reasonable assurances from the business associate that the PHI it receives will be safeguarded appropriately. To satisfy this requirement, in most cases, the covered entity must enter into a written agreement with the business associate specifying the purposes for which the PHI will be used or disclosed.

Given that covered entities do not typically perform all business functions "in house," but rather use billing services, utilization review companies, third party administrators and the like, it is reasonable to assume that virtually every covered entity has at least one business associate with whom it will need to enter into a written agreement. While entering into one agreement may not seem like a burden, other covered entities may have hundreds, if not thousands, of business associates with whom they must contract. Under the Privacy Regulation, all agreements with business associates were required to be in place by April 14, 2003 (the compliance date). This meant that even if any existing agreement between, for example, a covered entity and a billing service was not expiring prior to that date, the agreement would need to be amended to comply with the business associate requirements. Such an amendment process could have opened up many agreements to renegotiation at very inopportune times.

Extension of Compliance Deadline

The Proposed Rule addresses this concern by providing an extended compliance period for covered entities, other than small health plans (which were already granted a one-year extension), that have existing agreements with business associates, even if such agreements do not comply with the business associate agreement requirements of the Privacy Regulation. Specifically, the Proposed Rule extends the compliance period for existing agreements until, at the latest, April 14, 2004. However, if an agreement comes up for renewal or is modified prior to the 2004 date, provisions must be added to the agreement at that time to comply with the business associate requirements. An agreement that automatically renews (contains a so-called evergreen provision) will not be deemed to have been renewed as of the deemed renewal date, and thus covered

entities will have until April 14, 2004 to amend evergreen contracts (that are not otherwise modified prior to that date). Oral agreements are not eligible for the extended compliance period. In addition, covered entities that enter into new contracts (as opposed to renewing or modifying existing contracts) after the effective date of the Proposed Rule would be required to comply at that time with the business associate contract provisions in the Privacy Regulation. The extension does not affect a covered entity's responsibility to make PHI available to HHS (even if it is held by a business associate), to make PHI available (even if held by a business associate) to individuals for review and amendment or to give an accounting of uses or disclosures of PHI (including that held by a business associate).

In order to further assist covered entities in entering into agreements with business associates, the Proposed Rule contains model language that can be used to frame a business associate agreement. The Proposed Rule makes it clear that covered entities are not required to use the model language and that the language proposed is not intended to make up a complete agreement. However, the publication of model language may make compliance with the written agreement requirement somewhat simpler. In fact, in the case of existing agreements, covered entities may choose to simply use the model language as an addendum to the agreement.

Other Obligations of Business Associates

The Privacy Regulation requires that a covered entity be diligent in ensuring that a business associate not misuse PHI. The broad language used in the Privacy Regulation raised a concern among many covered entities that they would have to actively monitor their business associates in order to comply with the Privacy Regulation. The Proposed Rule reiterates a point made in guidance issued last summer that covered entities are not required to actively monitor their business associates and generally will not be held liable for their misdeeds. Rather, if a covered entity *knows* of a pattern of misdeeds that breaches the business associate's obligations, the covered entity must take steps to cure or end the violation or, if not curable (or cured), to terminate the agreement with the business associate or notify HHS where termination is not feasible.

The Privacy Regulation requires covered entities that act as business associates to enter into business associate agreements with respect to such activities. While many believed this was unnecessary, due to the fact that a covered entity is already obligated, by virtue of its status, to maintain the confidentiality of PHI, the Proposed Rule reiterates the requirement and points out that it is important to delineate permissible uses of PHI by business associates, and ensure that disclosure is only made for those purposes, including by covered entities. Thus, covered entities will continue to need to evaluate their operations to determine if they are providing services as business associates, (*e.g.,* hospitals that bill for certain physician practice), and in such cases enter into business associate agreements that comply with the requirements of the Privacy Regulation.

Conclusion

It is clear that while the provider community welcomes most of the changes, consumer advocates have concerns that the changes may not adequately protect the privacy rights of patients. The elimination of the consent requirement seems likely to be especially controversial. At least one Congressional committee, the Senate Health, Education, Labor, and Pensions Committee, chaired by Senator Edward Kennedy (D-MA), has already scheduled hearings on the new Proposed Rule. All of this seems to guarantee that the last chapter has yet to be written in the never-ending HIPAA story.

For further information about HIPAA, please contact the Mintz Levin attorney with whom you have a relationship, or Ellen Janos in the Boston office: 617 348 1662 / ejanos@mintz.com; or Peter Kazon in the Washington, D.C. office: 202 661 8739 / pkazon@mintz.com.

MINTZ LEVIN COHN FERRIS GLOVSKY AND POPEO PC

www.mintz.com

One Financial Center
Boston, Massachusetts 02111
617 542 6000
617 542 2241 fax

701 Pennsylvania Avenue, N.W.
Washington, D.C. 20004
202 434 7300
202 434 7400 fax

11911 Freedom Drive
Reston, Virginia 20190
703 464 4800
703 464 4895 fax

666 Third Avenue
New York, New York 10017
212 935 3000
212 983 3115 fax

157 Church Street
New Haven, Connecticut 06510
203 777 8200
203 777 7111 fax