

Healthcare

SPECIAL REPORT

A Publication of Morris, Manning & Martin, LLP

July 2001, Special Edition

*** DHHS CLARIFIES PRIVACY RULE ***

What is it? In the comments to the final Privacy Rule, published on January 4, 2001, the Department of Health and Human Services (“DHHS”), promised to publish guidance to assist those required to comply with the Rule. DHHS issued the first such guidance on July 6, 2001 which is intended to clarify the Privacy Rule and “correct any unintended negative effects” in an effort to help those who must comply with the Rule by its April 14, 2003 deadline.

What does it mean for me? The Guidance is intended to lift any barriers to access to or delivery of quality healthcare created by the Rule. For providers, it gives practical guidance on dealing with privacy issues in the following critical areas: obtaining patient consents; setting appointments and scheduling surgery; communicating with patients, family and staff; maintaining patient sign-in sheets; maintaining patient records (both in the office and in the hospital); teaching medical students and personnel; obtaining consults; filling prescriptions; rendering emergency services; when to use consents and/or authorizations; and limiting the need to redesign office space and computer systems.

Where can I find more information about the Privacy Rule or the Guidance? A summary and discussion of the Final Privacy Rule can be found at <http://mmmlaw.com/practices/healthcare/newsletters/winter01/index.html>). The Guidance is discussed in detail below. Please contact any of the members of our healthcare practice listed on page 8 of this Special Report for additional information or advice concerning your privacy and security concerns.

HIPAA Privacy Compliance Countdown: 20 Months 89 Weeks 623 Days

DHHS Issues Its First HIPAA Privacy Guidance

By Kimberly B. Greaves

OVERVIEW

The Guidance addresses some of the most frequently asked questions found in the more than 11,000 public comments to the final Rule received by DHHS during a 30-day comment period this past March. The Guidance also identifies areas of the Privacy Rule where DHHS recognizes a modification or change is necessary and intends to propose such amendments. Throughout the Guidance, DHHS emphasizes areas where the Rule’s requirements are scalable, allowing providers and payers the flexibility to create their own privacy procedures which can be “tailored to fit their size and needs.” The key areas addressed in the Guidance include consent, the minimum necessary standard, oral communications, business associates, parents and minors, health-related communications and marketing, research, and payments.

Changes or clarifications to the Rule to be proposed by DHHS

- Pharmacists may fill physicians’ phone-in prescriptions before obtaining patient consent.

Upcoming HIPAA Events

August 5, 2001 Ms. Sidney Summers Welch will speak at the Medical Association of Georgia Legislative Session at Amelia Island, on “What is this ‘HIPPO’ I Keep Hearing About? An Informative Discussion of the Coming HIPAA Regulations and How They Will Affect the Practice of Medicine in Your Office.”

August 23-24, 2001 Rick Haury, will speak at the annual meeting of the NC Association of CPAs in Greensboro, NC on “Creating New Opportunities Through the Internet - an Update”

August 2001 - Watch for the Summer 2001 Healthcare Update featuring the latest news in healthcare law, including HIPAA Privacy Developments.

Fall 2001 -HIPAA Privacy Compliance Seminar, “How to avoid the HIPAA stampede.” Date to be announced.

Continued on page 2

THE HIPAA UPDATE:

Continued from page 1

- Providers to whom a patient has been referred for the first time, may use personal health information to set up appointments or schedule procedures without first obtaining a consent.
- Covered entities may still engage in communications necessary for “quick, effective, high quality healthcare,” including routine oral communications with family and staff, telephone discussions with the patient or a family member over the phone, and calling out a patient name in waiting areas.
- Common practices such as patient sign-in sheets, x-ray light boards and bedside medical charts are not prohibited.

CONSENT

In addition to or apart from the medical records release that providers are accustomed to obtaining in accordance with state laws, the Privacy Rule requires providers to obtain a signed, written consent from the patient that meets certain requirements (“Consent”) in order to use and disclose in order to use and/or disclose protected health information described by the Rule (“PHI”) for purposes of treatment, payment, or healthcare operations (“TPO”). To address the many concerns regarding obtaining consent and the potential impact of the consent requirement DHHS offered the following clarifications:

Consents required in direct vs. indirect treatment relationships

- Health plans and clearinghouses may use and disclose PHI for TPO purposes without obtaining a patient consent; whereas healthcare providers with a direct treatment relationship must always obtain a consent. Generally, a “direct treatment provider” is one that treats a patient directly, rather than based on the orders of another provider, and/or provides healthcare services or test results directly to patients. However, if health plans or clearinghouses choose to obtain a consent, the consent must meet the standards, requirements, and implementation specifications for consents under the Rule.
- Under the current version of the Privacy Rule, direct treatment providers, such as a specialist or hospital, to whom a patient is referred for the first time, may not use the patient’s PHI to set up appointments or schedule surgery or other procedures before obtaining the patient’s written consent. DHHS noted that this was not the intended effect and, therefore, the Secretary will propose modifications to the Rule to address this problem.
- A provider with a direct treatment relationship with the patient must initially obtain a consent to use the patient’s PHI for treatment purposes, but when such provider consults with another healthcare provider about the patient’s case, additional consent is not required because such consultation falls within the definition of “treatment.” However, once the consulting provider engages in a direct treatment relationship with such patient, an additional consent will be necessary.

Effect on pharmacy services

- A strict reading of the Privacy Rule would prevent a pharmacist from filling a prescription that has been telephoned in by the patient’s physician if the patient is a new patient to the pharmacy and has not previously provided a written consent to the pharmacy. Not intending for the Privacy Rule to interfere with pharmacists activities in this way, the Secretary of HHS intends to propose modifications to the Rule to address this limitation and ensure that patients have access to call-in prescription services.
- Additionally, a pharmacist may provide advice about over the counter medicines without obtaining the customer’s prior consent, provided the pharmacist does not create or keep the record of any PHI.
- A pharmacist may use professional judgment and experience with common practice to make reasonable inferences of the patient’s best interest to allow a person, other than the patient, to pick up a prescription.

Obtaining consent in emergency situations

- When determining whether an emergency situation exists that warrants foregoing the attainment of a consent prior to treatment, the healthcare provider is advised to exercise his professional judgment to determine whether obtaining a prior consent would interfere with the timely delivery of necessary healthcare. Upon such determination, the provider may use or disclose PHI that was obtained during the emergency treatment, without a prior consent, to carry out TPO. However, the provider must attempt to obtain a consent as soon as reasonably practicable after the provision of treatment.

No conflict with ADA or Title VI

- The Privacy Rule includes an exception to the consent requirement allowing a provider to use his professional judgment as to whether consent can be obtained due to substantial barriers to communication with the individual. The Guidance clarifies that this exception does not affect covered entities’ obligations under Title VI or the ADA. Entities that are covered by these statutes must continue to meet the requirements of these laws. It is the intent of the Privacy Rule to work in conjunction with these laws to remove impediments to access to necessary healthcare for all individuals.

Consents vs. Authorizations

- A healthcare provider is required to obtain a consent from a patient for all uses or disclosures of PHI for TPO purposes only one time, whether there is a connected course of treatment or treatment for unrelated conditions. A healthcare provider needs only to obtain a new consent from a patient if the patient has revoked the consent between treatments.
- Compared to a consent, an authorization is much more specific and gives a covered entity permission to use designated PHI for specified purposes. An authorization is required for each use and disclosure of PHI not otherwise allowed by the Rule. In general, this means an authorization is required for purposes that are not part of TPO and not described in § 164.510 (uses and disclosures that require an opportunity for the individual

Continued on page 3

THE HIPAA UPDATE:

Continued from page 2

to agree or to object) or § 164.512 (uses and disclosures for which consent, authorization, or an opportunity to agree or to object is not required).

- All covered entities, not just direct treatment providers, must obtain an authorization to use or disclose PHI for any purpose not otherwise allowed by the Rule (whereas only direct treatment providers are required to obtain a consent).
- A covered entity will never need to obtain both an individual's consent and authorization for a single use or disclosure. However, a provider may have to obtain a consent and an authorization from the same patient for different uses or disclosures. For example, an obstetrician may, under the consent obtained from the patient, send an appointment reminder to the patient, but would need an authorization from the patient to send her name and address to a company marketing diaper services.

Consents held by other covered entities or affiliated entities

- Healthcare providers are not required to determine whether another covered entity has a more restrictive form of consent before disclosing PHI to that covered entity for TPO purposes.
- Additionally, one covered entity is not bound by a consent obtained by another covered entity, or any restrictions on such consent, unless the two covered entities have chosen to use a "joint consent." Affiliated entities are considered to be one entity under the Privacy Rule and, therefore, only one consent is needed for use by all affiliated entities and each such entity is bound by that one consent.
- If healthcare providers are affiliated or part of an organized healthcare arrangement located in different states with different laws regarding uses and disclosures of health information, the Privacy Rule does not require that the providers in each state obtain a consent from the patient who wishes to obtain treatment from these providers. Further, the Privacy Rule does not require that the consent include any details about state law and, therefore, does not require different consent forms in each state. [However, healthcare providers should keep in mind that state law may impose additional requirements for consent forms].

Format of consents/signature requirements

- A covered entity may choose to obtain and store consents in paper or electronic form, provided that the consent meets all the requirements under the Privacy Rule, including that the consent must be signed by the patient.
- A covered entity is not required to verify a signature on a consent form in the event that the individual signs the consent without someone from the covered entity present.

Effect of patient's revocation of consent on provider's billing for services

- A healthcare provider that provides a healthcare service to an individual after obtaining a consent from such individual, may bill for such service even if the individual immediately revokes the consent after the service has been provided. Although

individuals have the right to revoke consents, to the extent that the healthcare provider has relied upon the consent, the revocation is not effective. Therefore, in the case where a provider has obtained a consent and provided services pursuant to such consent with the expectation that he or she could bill and collect for the service provided, the healthcare provider has acted in reliance on the consent and consequently revocation would not be effective. However, after the healthcare provider has billed and collected for the services rendered in reliance on the consent, he or she may not make any further use or disclosure of the PHI for TPO or any other purpose. Revocations must be in writing to be effective.

Using consents obtained prior to the compliance deadline

- If a provider obtained a consent for the use or disclosure of health information for any one of the TPO purposes prior to the compliance date (April 14, 2003), the provider may use the health information collected pursuant to that consent for all three (3) purposes after the compliance date. Thus, a provider that obtained consent for use or disclosure for billing purposes would be able to draw on the data obtained prior to the compliance date and covered by the consent form for all TPO activities to the extent not expressly excluded by the terms of the consent.

THE MINIMUM NECESSARY STANDARD

DHHS also addressed and clarified issues pertaining to the "minimum necessary standard." In general, the Privacy Rule requires covered entities to take reasonable steps to limit the use or disclosure of, and requests for PHI to the minimum necessary to accomplish the intended purpose. The Privacy Rule obligates the covered entity to develop and implement policies and procedures that identify the persons or classes of persons within the covered entity who need access to PHI to carry out their job duties, the categories or types of PHI needed by these persons or classes of persons, and conditions appropriate to such access. For example, a hospital might implement policies that permit doctors, nurses or others involved in treatment to have access to the entire medical record, as needed. A case-by-case review of each use is not required, but the covered entity's written policies and procedures must state that access to the entire medical record by certain persons or classes of persons is necessary and include a justification for such broad access.

The Guidance also states that in certain circumstances, a covered entity may rely on the judgment of the party requesting the disclosure as to the minimum amount of information that is needed, so long as such reliance is reasonable under the particular circumstances of the request. This "reasonable reliance" is permitted for a request made by a public official or agency for a permitted disclosure under the Rule, another covered entity, a professional who is a workforce member or business associate of the covered entity and a researcher with appropriate documentation from an Institutional Review Board.

Continued on page 4

THE HIPAA UPDATE:

Continued from page 3

DHHS addressed the following concerns about the application of the minimum necessary standard in treatment settings where medical information must be conveyed freely and quickly:

Covered entities only required to take reasonable steps

- Recognizing that covered entities will need flexibility to address their unique circumstances, the Privacy Rule imposes a reasonableness standard allowing covered entities to make their own assessment of what PHI is reasonably necessary for a particular purpose, given the characteristics of the covered entity's business and workforce, and to implement policies and procedures accordingly. This is not a strict standard and covered entities need not limit information uses or disclosures to those that are absolutely needed to serve the purpose. Rather they should employ an approach consistent with the best practices and guidelines already used by many providers already to limit the unnecessary sharing of medical information.

Major redesigns of workflow and computer systems not needed

- In response to the numerous concerns that the requirements to limit access to PHI would require covered entities to completely restructure existing workflow systems, including redesigns of office space and upgrades of computer systems, DHHS stated that the basic minimum necessary standard requires only that covered entities make reasonable efforts to limit access to PHI to those in the workforce that need access based on their roles in the covered entity. Further, DHHS does not consider facility redesigns necessary to meet the reasonableness standard for minimum necessary uses. Rather, covered entities may simply need to make certain adjustments to their facilities to minimize access, such as isolating and locking file cabinets or records rooms, or providing additional security, such as passwords, on computers maintaining PHI. The Guidance suggests that DHHS will take into account a covered entity's resources and abilities to configure their record systems to limit access, and the practicality of organizing systems to allow this capacity. For example, it may not be reasonable for a small, solo practitioner who has a largely paper-based records system to limit access of employees with certain functions to only limited fields in a patient record, while other employees have access to the complete record. Alternatively, a hospital with an electronic patient record system is more likely to be able to reasonably implement such controls, and would more likely be expected to do so.

Sign-in sheets, beside charts and x-ray light boards still permissible

- And dispelling perhaps some of the most prolific myths circulating in HIPAA discussions, the Guidance provides that the minimum necessary requirements are not intended to prohibit covered entities from maintaining patient medical charts at bedsides, require that covered entities shred empty prescription vials, require that x-ray light boards be isolated or prohibit the use of sign-in sheets in waiting rooms. Again,

DHHS emphasized that the Privacy Rule simply imposes on the covered entity the obligation to take reasonable precautions to prevent inadvertent or unnecessary disclosures. DHHS intends to propose modifications to the Privacy Rule to increase covered entities' confidence that these practices are not prohibited.

Medical residents and students access to PHI not prohibited

- The minimum necessary standard does not prohibit healthcare providers from disclosing PHI to medical residents, medical students, nursing students and other medical trainees in the course of their training.

Authorizations from third parties acceptable

- Minimum necessary determinations are not required where an authorization is given by an individual, even if the authorization was given to the third party and then conveyed to the covered entity. For example, life, disability or casualty insurers may request information from the healthcare provider by submitting the patient's application for a claim under an insurance policy as the necessary authorization. However, the authorization must meet the requirements of the Privacy Rule. But note, the minimum necessary standard will apply to authorizations requested by the covered entity for its own purposes.

Disclosures to State or Federal Agencies only with authorization

- Requests for disclosure of PHI by federal or state agencies, such as the Social Security Administration, must be authorized by an individual and, therefore, will not require the covered entity to make a minimum necessary determination before disclosing information to such agencies. Further, providers can accept the agency's authorization form as long as it meets the requirements of the Privacy Rule.

No conflict with Transactions Standards

- For those ahead of the curve and already addressing the requirements of the Transactions Standards, the Guidance clarifies that the minimum necessary standard does not conflict with the Transactions Standards because the Privacy Rule exempts from the minimum necessary standard any uses or disclosures that are required for compliance with the applicable requirements of the subchapter, which includes all data elements that are required or situationally required in standard transactions. However, the minimum necessary standard will apply to optional data elements in the Transactions Standards.

ORAL COMMUNICATIONS

The Privacy Rule applies to individually identifiable health information in all forms, electronic, written, oral and any other. The Guidance clarifies that oral communications shall be treated like any other form and, therefore, covered entities must reasonably safeguard PHI from any intentional or unintentional use or disclosure that is in violation of the Rule. Consequently, covered entities must have in place appropriate administrative, technical

Continued on page 5

THE HIPAA UPDATE:

Continued from page 4

and physical safeguards to protect the privacy of PHI, including oral information. Yet at the same time, DHHS understands that oral communications must occur freely and quickly in treatment settings and, therefore, DHHS addressed concerns with respect to these communications as follows:

Common communication practices still permissible

- The Privacy Rule is not intended to prevent confidential conversations between healthcare providers or between providers and patients, even if there is a possibility that such conversations may be overheard. The following practices would be considered permissible, if reasonable precautions are taken to minimize the chance of inadvertent disclosures to others who may be nearby (such as using lowered voices or talking apart from others):
 - Healthcare staff may orally coordinate services at hospital nursing stations.
 - Healthcare professionals may discuss a patient's condition over the phone with the patient, a provider or a family member.
 - A healthcare professional may discuss lab test results with a patient or other provider in a joint treatment area.
 - Healthcare professionals may discuss a patient's condition during training rounds in an academic or training institution.

DHHS plans to propose regulatory language to reinforce and clarify that these and similar oral communications (such as calling out patient names in a waiting room) will be considered permissible under the Privacy Rule.

Significant office or facility redesigns not necessary

- The Privacy Rule does not require hospitals and doctors' offices to be "retrofitted," to provide private rooms and soundproof walls to avoid any possibility that a conversation is overheard. Reemphasizing the use of a reasonableness standard, the Guidance states that the covered entity is required to "reasonably safeguard" against uses or disclosures not permitted by the Rule, but this does not mean that the covered entity must guarantee the privacy of PHI from any and all potential risks. In determining what is reasonable, DHHS will take into account the concerns of covered entities regarding potential effects on patient care and financial burden. Covered entities will need to review their own practices and determine what steps are reasonable to safeguard patient information. DHHS gave the following as examples of modifications to facilities or systems that may constitute reasonable safeguards:
 - Pharmacies could ask waiting customers to stand a few feet back from a counter used for patient counseling.
 - Providers could add curtains or screens to areas where oral communications often occur between doctors and patients or among professionals treating the patient.
 - Providers could install cubicles, dividers, shields or similar barriers where multiple patient-staff communications routinely occur.

Covered entities are advised to consider the viewpoint of a prudent professional in determining what is "reasonable."

BUSINESS ASSOCIATES

In general, the Privacy Rule requires covered entities to obtain "satisfactory assurances" from the covered entity's business associates that the associate will use the information only for the purposes for which they were engaged by the covered entity, will safeguard the information from misuse and will help the covered entity comply with the covered entity's duties to provide individuals with access to health information about them and a history of certain disclosures. The Guidance emphasizes that PHI may be disclosed to business associates *only* to help the providers and plans carry out their healthcare functions — not for independent use by the business associate. DHHS clarifications regarding the requirements related to business associate relationships include the following:

Rule does not apply to business associates

- The Privacy Rule does not apply to business associates. The assurances that covered entities must obtain prior to disclosing PHI to business associates create contractual obligations much narrower than the provisions of the Rule which protect information generally and help the covered entity comply with its own obligations under the Rule.

Covered entities are generally not liable for business associates' actions

- Covered entities are not liable for privacy violations of their business associates, nor are they required to actively monitor or oversee the safeguards or other measures implemented by the business associate to comply with the requirements of the contract. Moreover, a business associate's violation of the term of its contract with a covered entity does not, in and of itself, constitute a violation of the Rule by the covered entity, but the contract must obligate the business associate to notify the covered entity when violations have occurred. Once a covered entity becomes aware of a pattern or practice of a business associate that constitutes a material breach or violation of the business associate's obligation under its contract, the covered entity is obligated to take "reasonable steps" to cure the breach or to end the violation. Reasonable steps will vary with the circumstances and nature of the business relationship. If such steps are not successful, the covered entity must terminate the contract if feasible. If termination is not feasible, for example where there are no other viable business alternatives, the covered entity must report the problem to the DHHS. If, and only if, the covered entity fails to take such steps as described above will it be considered to be out of compliance with the requirements of the Rule.

PARENTS AND MINORS

Parents and guardians have right of access to PHI

- Consistent with the Privacy Rule's general premise that individuals have certain rights with respect to their PHI,

Continued on page 6

THE HIPAA UPDATE:

Continued from page 5

including the right to obtain access to their PHI, a parent is generally considered the personal representative of his or her minor child and, therefore, has the right to such access. The Guidance clarifies that this will also extend to a guardian or other person acting *in loco parentis* of a minor. However, the Privacy Rule also expressly states that it does not preempt state laws that specifically address disclosure of health information about a minor to a parent. This is true whether the state law authorizes or prohibits such disclosure. Thus, a provider may comply with a state law that requires disclosure to a parent and would not have to accommodate a request for confidential communications that would be contrary to state law.

Limitations on parent's or guardian's access to PHI

- A parent's right to access his or her children's PHI is subject to two (2) exceptions. The first occurs when the parent agrees that the minor and the healthcare provider may have a confidential relationship. In such case the provider is allowed to withhold information from the parent to the extent of that agreement. The second exception arises when the provider reasonably believes in his or her professional judgment that the child has been or may be subjected to abuse or neglect, or that treating the parent as the child's personal representative could endanger the child. Secretary Thompson has stated that he is reassessing these provisions of the Privacy Rule.

HEALTH-RELATED COMMUNICATIONS AND MARKETING

The Guidance notes that the Privacy Rule sets limits on the kind of marketing that can be done as part of a covered entity's healthcare operation and requires individual authorization for all other uses or disclosures of PHI for marketing purposes. For purposes of the Privacy Rule "marketing" is defined as "a communication about a product or service, a purpose of which is to encourage recipients of the communication to purchase or use the product or service."

What "Marketing" is not

A covered entity is not "marketing" when it:

- Describes the participating providers or plans in a network.
- Describes the services offered by a provider or the benefits covered by a health plan.
- Communicates an individual's PHI as part of the provider's treatment of the patient or for purposes of furthering that treatment.
- Communicates PHI to an individual when such communication is made in the course of managing the individual's treatment or recommending alternative treatment.

Authorizations for marketing required

- The Rule is not intended to expand the ability of providers, plans, marketers and others to use PHI to market goods and services. The Privacy Rule requires the patient's authorization for the following types of uses or disclosures of PHI for marketing:

- Selling PHI to third parties for their use and re-use. For example, a hospital or other provider may not sell names of pregnant women to baby formula manufacturers or magazines.
- Disclosing PHI to outsiders for the outsiders' independent marketing use. For instance, doctors may not provide patient lists to pharmaceutical companies for those companies' drug promotions.
- Telemarketers may not gain access to PHI unless the covered entity obtains the individual's authorization to do so. Additionally, in such cases a telemarketer must be a business associate, which means that it must agree by contract to use the information only for marketing on behalf of the covered entity and not to market its own goods or services (or those of another third party). Further, the telemarketer must identify the covered entity that is sponsoring the marketing call and must also provide individuals the opportunity to opt-out of any future marketing efforts by the telemarketer.

Authorization exceptions

- An authorization is not required before a provider or health plan engages in marketing to an individual if:
 - The marketing occurs during an in-person meeting between the patient and provider or health plan representative.
 - The marketing concerns products or services of nominal value (but DHHS does not address what is "nominal value").
 - The covered entity is marketing health-related products and services (of either the covered entity or a third party), the marketing identifies the covered entity that is responsible and the individual is offered an opportunity to opt-out of future marketing. In addition, the marketing must (i) advise people if they have been targeted based on health status and (ii) if the covered entity is compensated (directly or indirectly) for making the communication.

RESEARCH

The Privacy Rule establishes the conditions under which PHI may be used or disclosed by covered entities for research purposes. A covered entity may always use or disclose for research purposes health information which has been de-identified in accordance with the Rule, and may also use and disclose PHI for research without individual authorization under limited circumstances set forth in the Privacy Rule.

Many people voiced concerns that the Rule would hinder medical research by making doctors and others less willing and/or able to share information about individual patients. DHHS states in the Guidance that they do not believe that the Privacy Rule will hinder medical research. In their opinion, patients and health plan members should be more willing to participate in research when they know that their information will be protected.

Continued on page 7

THE HIPAA UPDATE:

Continued from page 6

RESTRICTIONS ON GOVERNMENT ACCESS TO HEALTH INFORMATION

Perhaps in a show of fairness (or a challenge that if government agencies can comply anyone can), the Privacy Rule requires government-operated health plans and healthcare providers to meet substantially the same requirements as private ones for protecting the privacy of individually identifiable health information. Addressing concerns however about government access to PHI, DHHS provided the following guidance:

Government access to PHI for compliance monitoring

- The Rule does not require a physician or any other covered entity to send medical information to the government for a government database or similar operation. However, the Rule does give DHHS the authority to investigate complaints and to otherwise ensure that covered entities comply with the Rule, which may require DHHS to access certain PHI. The Privacy Rule limits disclosure to DHHS to information that is “pertinent to ascertaining compliance.” DHHS is obligated to maintain stringent controls to safeguard any individually identifiable health information that it receives.

Law enforcement’s access to PHI

- The Privacy Rule establishes new procedures and safeguards to restrict the circumstances under which a covered entity may give PHI to law enforcement officers. Further, even when disclosure to law enforcement is permitted by the Privacy Rule, covered entities are not *required* by the Rule to disclose any information. However, where state law imposes additional restrictions on disclosure of health information to law enforcement, those state laws will continue to apply.

No conflict with state law disclosure requirements

- Recognizing that virtually all states have laws that require providers to report cases of specific diseases to public health officials, the Privacy Rule does not prohibit or interfere with such disclosures, nor other disclosures also permissible under the Privacy Rule. The Privacy Rule also allows the continuance of the existing practice of sharing PHI with public authorities that are authorized by law to collect or receive such information to aid them in their mission of protecting the public health.

PAYMENT

Reporting delinquent payments to credit agencies

- Under the Privacy Rule, a covered entity may use and disclose PHI for payment purposes. In this regard, DHHS specifically states that the Privacy Rule will not prevent reporting to consumer credit reporting agencies, but such disclosures shall be limited to the following PHI about the individual: name and address; date of birth; social security number; payment history; account number. Additionally, disclosure of the name and address of the healthcare provider or health plan making the

report is allowed.

Use of collection agencies

- Covered entities will also be allowed to continue to use the services of debt collection agencies. Debt collection is recognized as a payment activity within the “payment” definition. Disclosures to collection agencies under a business associate agreement are governed by the provisions of the Rule, including consent (where consent is required) and the minimum necessary requirements. Due to the broad definition of “payment,” obtaining information about the location of an individual in order to facilitate collections would constitute a payment activity and be allowed under the Privacy Rule. The Privacy Rule does not conflict with or preempt the Fair Debt Collection Practices Act and, therefore, the covered entity and its business associates would also have to comply with any limitations placed on location information services by such Act.

Author’s note: The full text of the Privacy Rule and the July 6 Guidance can be accessed at <http://aspe.os.dhhs.gov/admnsimp/>. The DHHS Office of Civil Rights’ website at <http://www.hhs.gov/ocr/hipaa2.html> allows individuals to submit questions regarding the Privacy Rule, but answers will only be given in a “frequently asked questions” format on the OCR website. A summary of the Privacy Rule was published in the Winter 2001 MMM Healthcare Update which can be found at <http://mmmlaw.com/practices/healthcare/newsletters/winter01/index.html/>.

HIPAA Privacy Countdown

20 Months
89 Weeks
623 Days

Watch for more HIPAA bulletins
from MM&M with helpful tips on
how you can achieve HIPAA
Compliance.

MM&M Healthcare Attorneys

Tara L. Adyanthaya	(404) 504-7671	tadyanthaya@mmmlaw.com
Ward S. Bondurant	(404) 504-7606	wbondurant@mmmlaw.com
Kimberly B. Greaves	(404) 504-7634	kgreaves@mmmlaw.com
Richard L. Haury, Jr.	(404) 504-7713	rhaury@mmmlaw.com
Randall W. Johnson	(404) 504-7646	rjohnson@mmmlaw.com
Daniel J. Mohan	(404) 504-7610	dmohan@mmmlaw.com
John H. Northey III	(704) 554-7070	jnorthey@mmmlaw.com
L. Chris Peterson (D.C. Office)	(202) 408-5153	lpeterson@mmmlaw.com
Sidney Summers Welch	(404) 495-3658	swelch@mmmlaw.com
Robert C. Threlkeld	(404) 504-7757	rthrelkeld@mmmlaw.com

This newsletter is provided solely for informational purposes and presents only highly condensed summaries relating to the topics presented. Therefore, it should not be relied upon as a complete record for purposes of regulatory compliance, nor is it intended to furnish legal advice adequate to any particular circumstances. Addressees and other readers are urged to consult their attorneys and advisors about any questions they may have. For additional information on any of the topics in this newsletter, please contact the authors or Robert C. Threlkeld, newsletter editor.



1600 Atlanta Financial Center
3343 Peachtree Road, NE
Atlanta, GA 30326
Phone: (404) 233-7000
Facsimile: (404) 365-9532
E-Mail: Attorney Initials@mmmlaw.com

Webpage: www.mmmlaw.com

SUMMER 2001

Copyright © 2001 Morris, Manning & Martin, LLP