

HIMOS

& Health Plans

Spring 2002 Volume 5 Issue 1

A Publication of the American Health Lawyers Association HMOs and Health Plans Substantive Law Committee

TABLE OF CONTENTS

HIPAA Privacy Rule Breaking the Chain of Trust—How the Rule May Impede the Provision of Healthcare
Joshua Kaye, Esq.11

Denial of Claims for Coverage of Addictive Drugs: Best Practice or an Invitation for Liability?
Jennifer Philpot, Esq.29

Subrogation and Re-imbursment: *Great-West v. Knudson* was no Death Knell
Lisa Murphy, Esq.
Anthony Shelley, Esq.16

Expanding Individual Rights to Healthcare Information: The Information Requirements of the DoL Claims Procedures and the Designated Record Set Requirements of the HIPAA Privacy Standards
Donna O'Connor, Esq.20

The False Claims Act and Federal Managed Care Programs: Drawing the Battle Lines
Janet Nolan, Esq.
R. Jeffrey Layne, Esq.23

Fraudulent Foreign Claims Submitted to HMOs: Identification, Review, and Disposition
Alan Bloom, Esq.28

HIPAA Privacy Rule: Breaking the Chain of Trust—How the Privacy Rule May Impede the Provision of Healthcare

Joshua M. Kaye, Esquire
*McDermott Will & Emery
Miami, Florida*

I. Introduction

Healthcare is undergoing dramatic change as the industry shifts toward e-based business. Among the factors driving this transformation are pressures to cut costs by moving from paper-based to electronic processes and a growing demand by patients to receive higher quality healthcare. The impetus for these changes is the Health Insurance Portability and Accountability Act of 1996 (HIPAA),¹ which was enacted in some measure to address the fact that the country's 1,500 plus healthcare payors employed a large variety of formats and data requirements to handle healthcare claims and related transactions.² The lack of a single national standard has created a transaction environment that is unnecessarily costly and prone to errors.³ HIPAA was intended to reduce the administrative and transaction costs associated with the healthcare industry by requiring the industry to shift to fully interoperable systems for healthcare transactions, thus promoting efficient healthcare markets.⁴ As a by-product of a more uniform and efficient healthcare industry, it is

hoped that medical errors will decline thereby raising the quality of and access to healthcare in this country.⁵

At the same time, Congress recognized that the increasing complexity of the healthcare industry presented challenges to maintaining the confidentiality of individually identifiable health information, and thus authorized the Secretary of the Department of Health and Human Services (DHHS) to promulgate regulations for the privacy of individually identifiable health information.⁶ The privacy standards were published by the DHHS Secretary as final regulations on December 28, 2000, (the Privacy Rule) and the proposed modifications to the Privacy Rule were published March 27, 2002 (the Proposed Modifications). The regulation and proposed modifications require health plans, health maintenance organizations (HMOs), physicians groups, and others in the healthcare chain of trust to implement security measures that preserve the confidentiality of sensitive health information.

In enacting such security measures, however, the Privacy Rule ultimately will impede the delivery of quality healthcare because the Privacy Rule will disadvantage health plans, HMOs, health insurers, and others in the healthcare chain of trust, as well as associated business partners in at least three ways: (1) by the significant administrative costs and

burdens incurred by healthcare entities in implementing and maintaining compliance with the Privacy Rule; (2) by precluding the flow of essential healthcare communications among healthcare entities and healthcare professionals due to the fear of exposure to liability for improperly handling private health information; and (3) by the costs associated with lawsuits brought by individuals exploiting newly founded rights and claiming harms recognized at common law due to the misuse of protected health information.

This article is divided into the following parts: the first part begins with a discussion of the key concepts of the Privacy Rule including who falls within the jurisdiction of the regulations and to what does the Privacy Rule apply. The next part examines patients' rights under the Privacy Rule and provides a brief overview of enforcement and external sanctions. The next part focuses on how private health information may be used and disclosed for certain healthcare functions and specifically addresses the distinction between a "consent" and an "authorization". The final part scrutinizes the impact of the Privacy Rule on the collaboration of healthcare entities and other healthcare professionals and discusses how the health system chain of trust will be eroded because healthcare entities will (1) incur substantial and costly

Continued on page 2



HMOs and Health Plans © 2002 is published by the American Health Lawyers Association. All rights reserved. No part of this publication may be reproduced in any form except by prior written permission from the publisher. Printed in the United States of America. "This publication is designed to provide accurate and authoritative information in regard to the subject matter covered. It is provided with the understanding that the publisher is not engaged in rendering legal or other professional services. If legal advice or other expert assistance is required, the services of a competent professional person should be sought."
—from a declaration of the American Bar Association

Continued from page 1

administrative burdens to become compliant and maintain compliance with the Privacy Rule, (2) institute defensive information tactics causing a chilling effect on the collaboration among healthcare entities, and (3) be defending an onslaught of lawsuits, ultimately leading to a decline in the quality of and access to healthcare in this country.

II. Key Concepts

Understanding who must comply with the Privacy Rule requirements (a Covered Entity and their Business Associates) and to what sort of information the requirements apply (Protected Health Information) is the critical first step toward compliance with the Privacy Rule.

A. Covered Entities

Three categories of entities fall within the definition of a Covered Entity and are thus subject to the Privacy Rule. These entities are as follows: (1) a health plan⁷; (2) a healthcare clearing-house⁸; and (3) any healthcare provider⁹ who transmits any health information in electronic form in connection with a transaction covered by the Privacy Rule.¹⁰

As is evident from the definition of a Covered Entity, health plans and healthcare clearing-houses constitute Covered Entities by the very nature of their business operations. However, healthcare providers are not Covered Entities unless such providers transmit electronic health information in connection with a HIPAA transaction.¹¹ Accordingly, a provider that processes all of his or her

claims by paper or telephone would not be subject to the Privacy Rule. While unlikely, some small practitioners may find that their practices do not fall within the scope of the definition of a Covered Entity, and thus may be afforded some regulatory relief.

B. Protected Health Information

Protected Health Information (PHI) is defined as individually identifiable health information that is: (1) transmitted by electronic media; (2) maintained in any medium described in the definition of electronic media; or (3) transmitted or maintained in any other form or medium including oral communications or recorded transmissions.¹² As Donna Shalala, the former Secretary of the DHHS, explained:

Covering oral communications is an important part of keeping individually identifiable health information private. If the final rule were not to cover oral communications, a conversation about a person's protected health information could be shared with anyone. Therefore, the same protections afforded to paper and electronically based information must apply to verbal communications as well.¹³

By contrast, PHI does not include such items as cells and tissues.¹⁴ Nevertheless, any analyses of such items would fall within the scope of PHI.¹⁵ Similarly, physical items such as clothing or weapons like a bloody knife are not PHI, but the communications that accompany the use or disclosure of such items could constitute PHI.¹⁶ For example, if a physi-

cian provides cells to a researcher and the physician tells the researcher that these are cancer cells extracted from Jane Doe, while the cells are not PHI, the accompanying statement is PHI and must be treated accordingly under the Privacy Rule.¹⁷

C. Business Associates

The Privacy Rule requires that Covered Entities enter into written agreements with any Business Associates that receive PHI in the course of carrying out their treatment, payment, and healthcare operation (TPO) obligations for the Covered Entity.¹⁸ Generally speaking, there are two means by which an entity may fall within the definition of a Business Associate.¹⁹ First, a person constitutes a Business Associate when he, she, or it uses or discloses PHI that belongs to a Covered Entity to perform a function *on behalf of* the Covered Entity.²⁰ Second, those persons performing the services listed at 45 C.F.R. § 160.103 also may constitute Business Associates if the provision of such service involves the disclosure of PHI by the Covered Entity to the service provider.²¹ An example of the latter form of a Business Associate is a consultant to a Covered Entity who requires access to PHI belonging to the Covered Entity.²²

While healthcare providers and health plans may often find themselves entering into Business Associate arrangements, the Business Associate Rule does not apply to:

1. Disclosures by a Covered Entity including a healthcare provider to a healthcare provider concerning the treatment of an individual²³; and

2. Disclosures by a group health plan (or health insurance issuer or HMO with respect to a group health plan) to the plan sponsor if the requirements of 45 C.F.R. § 164.504(f) are met.²⁴

An analysis of the following two inquiries should aid in understanding who or what constitutes a Business Associate. First, must a physician enter into a Business Associate agreement with a health plan in order for such physician to disclose PHI to such health plan for TPO purposes? Second, does an insurer or HMO constitute a Business Associate where a group health plan purchases insurance or coverage from the same?

In addressing the former question, the answer is no such contractual arrangement is necessary because, while the physician may have an agreement to accept payment from the health plan as reimbursement for services rendered to subscribers of the health plan, the DHHS' position is that neither the healthcare provider nor the health plan are acting *on behalf of* or *providing a service to* the other.²⁵ Likewise in addressing the second question, the DHHS' position is that neither the health insurer nor HMO is a Business Associate of the group health plan, because the activities of the health insurer or HMO are on their own behalf and not on behalf of the group health plan.²⁶ Nevertheless, often a group health plan enters into an agreement with an HMO or health insurer to perform functions or to provide services that are in addition to the provision of insurance. In such a situa-

tion, the HMO or health insurer most likely would constitute a Business Associate.²⁷

Assuming a Business Associate relationship exists, the general rule is that a Covered Entity may disclose PHI to a Business Associate and may allow a Business Associate to create or receive PHI on behalf of the Covered Entity only if the Covered Entity obtains “satisfactory assurances” that the Business Associate will appropriately handle the PHI.²⁸ Satisfactory assurances means that Covered Entities must enter into a written agreement with each Business Associate explicitly requiring, among other things, for the Business Associate to: (1) use or disclose PHI in compliance with the Privacy Rule; (2) report any misuse of PHI to the Covered Entity; (3) impose the same requirements on the Business Associate’s agents; and (4) make an accounting of disclosures available to individuals.²⁹

While the Privacy Rule does not require Covered Entities to police the operations of its Business Associates, a Covered Entity may be held liable under the Privacy Rule if it actually knew of a material breach of the Privacy Rule by the Business Associate and failed to take steps to require a cure or to terminate the relationship.³⁰

III. Patients’ Rights; Sanctions

A. Patients’ Rights

The Privacy Rule provides patients with significant rights to learn about their own personally identifiable health information, and equally as important, to learn about the business and privacy practices

of the providers and plans from whom they obtain such health-care services. More specifically, the Privacy Rule establishes seven primary rights for individuals: (1) the right to notice of the entity’s privacy practices³¹; (2) the right to request restrictions on the use and disclosure of the individual’s PHI for TPO³²; (3) the right to receive confidential communications of the individual’s PHI³³; (4) the right to access the individual’s PHI³⁴; (5) the right to amend the individual’s PHI³⁵; (6) the right to an accounting of disclosures of the individual’s PHI³⁶; and (7) the right to complain to the Covered Entity and the DHHS Secretary about the privacy policies and procedures of an entity.³⁷

The administrative burdens associated with implementing such policies and procedures will be significant. Of particular interest are the convoluted notice requirements related to group health plans. Specifically, individuals who receive health benefits under a group health plan other than through insurance are entitled to receive a privacy notice from the group health plan.³⁸ By contrast, a group health plan is not required to maintain or provide a privacy notice where the group health plan provides health benefits through an insurance contract with a health insurer or HMO and the only PHI the group health plan creates or receives is summary information and information about an individual’s enrollment or disenrollment.³⁹ Nevertheless, under this latter scenario, if the group health plan creates or receives PHI, the group health

plan must maintain a privacy notice that it is required to distribute upon request.⁴⁰ In such a case, the individual is entitled to receive notice of the health insurer’s or HMO’s privacy practices but not those of the group health plan unless otherwise requested.

These notice requirements serve as but one example of the complex operational specifications that Covered Entities must implement with precise operational processes and controls to ensure compliance with the Privacy Rule. As further discussed below, these rights ultimately will hinder healthcare as exorbitant administrative costs are incurred by Covered Entities and the plaintiffs’ bar begins to exploit such rights in litigation.

B. Enforcement and Sanctions

The DHHS Secretary delegated enforcement of the Privacy Rule to the Office for Civil Rights (OCR). The OCR’s responsibilities include working with Covered Entities to secure voluntary compliance, investigating complaints, and, where voluntary compliance is unachievable, imposing civil monetary penalties.⁴¹ While the Privacy Rule apparently seeks to ease Covered Entities’ concerns by calling for the cooperation of the DHHS Secretary and Covered Entities to obtain voluntary compliance, non-compliance with the Privacy Rule should not be overlooked as it can result in hefty monetary fines as well as imprisonment.

In particular, the Privacy Rule provides for civil penalties of up to \$100 per person per violation or \$25,000 per person for the negligent violation of a single

standard in a year.⁴² The DHHS also may refer a matter to the Department of Justice to pursue criminal sanctions against any person who knowingly violates a standard.⁴³ A person or entity that knowingly commits a violation of the Privacy Rule may be fined up to \$50,000 and/or face imprisonment for a term not to exceed one year.⁴⁴ A person or entity that violates the Privacy Rule under false pretenses faces fines of up to \$100,000 and/or a term of imprisonment not to exceed five years.⁴⁵ The Privacy Rule further authorizes fines of up to \$250,000 and/or a term of imprisonment not to exceed ten years for any person who violates any standard with the intent to sell, transfer, or use PHI for commercial advantage.⁴⁶ Because the Privacy Rule authorizes such stringent penalties, it is important that Covered Entities understand how they may use and disclose PHI.

IV. Uses and Disclosures of PHI

This final part explains how PHI may be used and disclosed for certain healthcare functions and specifically addresses the distinction between a “consent” and an “authorization.”

A. Consent

The Privacy Rule generally permits Covered Entities to use and disclose PHI as necessary for TPO purposes.⁴⁷ Furthermore, the Privacy Rule permits two types of Covered Entities (i.e., health plans and health clearinghouses) to use or disclose PHI without obtaining a consent from the individual for the release of information for TPO.⁴⁸ Thus, a legal presumption exists that all

Continued on page 4

Continued from page 3

individuals have consented to the use and disclosure of their PHI by health plans and clearinghouses for purposes of TPO. In contrast, the third type of Covered Entity (i.e., healthcare providers) must obtain an individual's consent prior to using or disclosing such individual's PHI for TPO purposes.⁴⁹

The consent requirement only applies to uses and disclosures of PHI for TPO purposes. For any other use or disclosure, a Covered Entity must obtain an individual's specific authorization. Such authorization must be separate from the consent.

B. Authorization

In order to disclose PHI for a purpose other than TPO, Covered Entities must obtain an individual's authorization.⁵⁰

One major distinction between an authorization and a consent is that, while a Covered Entity may refuse TPO where an individual refuses to execute a consent, Covered Entities are prohibited from conditioning treatment, payment, or eligibility for benefits on obtaining an authorization.⁵¹ Accordingly, the authorization's purpose is aimed at preventing Covered Entities from coercing individuals into agreeing to the use or disclosure of such individual's PHI in a manner that is not necessary for such individual's healthcare.

Specifically, the core elements of an authorization include detailed information with respect to the use or disclosure and provide the individual fair notice about his or her rights with respect to an authorization and the potential for the information to be re-disclosed.⁵² In

addition to the core elements, certain additional provisions must be included under the following three sets of implementation specifications: (1) authorizations requested by a Covered Entity for its own uses or disclosures;⁵³ (2) authorizations requested by a Covered Entity for disclosures by others;⁵⁴ and (3) authorizations for research that includes treatment.⁵⁵

The effect of separating a consent from an authorization is that the distinct authorization should allow an individual to focus on any uses and disclosures that are not for TPO purposes. Accordingly, the authorization should permit individuals specifically to understand how and by whom their PHI is being utilized.⁵⁶

V. Burdens of the Privacy Rule

A. Administrative Burdens

The administrative burdens that the Privacy Rule places upon Covered Entities are too numerous to catalog. Nevertheless, it is worth highlighting a number of issues because of the negative impact they will have on the collaboration among healthcare organizations and others in the healthcare chain of trust.

For example, while the consent requirement arguably adds to a patient's understanding of a healthcare provider's privacy practices, it also will impede access to, and delivery of, quality healthcare. The consent requirement impedes the collaboration among healthcare entities and providers because an array of circumstances exists where healthcare providers need to use or disclose PHI for TPO purposes to others in the chain of trust prior to the initial face-to-face contact

with the patient and thus prior to obtaining consent. The current Privacy Rule does not permit these routine and often essential activities until the patient executes the necessary consent.⁵⁷ The consent requirement also will hinder the operations of hospitals that routinely utilize information received from a referring physician to schedule and prepare for the necessary procedure prior to the time the patient actually arrives at the hospital to execute the consent. To obtain a consent from such individual prior to using or disclosing his or her PHI creates a serious impediment to such activities.

The difficulties that will arise from healthcare organizations attempting to track consents will further impede medical treatment. Because the Privacy Rule permits an individual to revoke his or her consent, larger institutional providers may be exposed to the potential liability of using or disclosing PHI in reliance on a revoked consent. Accordingly, healthcare providers will be forced to undertake the associated expenses and administrative difficulties of either tracking patients' consents and revocations or obtaining a consent during each patient encounter. Additional dilemmas may arise where a patient revokes his or her consent because healthcare organizations may have to eliminate all PHI concerning such individual from their information technology systems in order to ensure that the PHI is not used inadvertently or improperly. Because such PHI is often used by healthcare entities to evaluate and improve healthcare operations, such elimination could significantly deter quality improvement activities.

It is worth noting that the DHHS is attempting to address many of these administrative concerns. Specifically, the Proposed Modifications remove the requirement to obtain consent prior to receiving initial treatment from a healthcare provider.⁵⁸ Instead, patients would be asked to acknowledge a privacy notice, but healthcare providers could treat such patients even if the patient did not make such acknowledgement.⁵⁹ This change would allow patients to consider a provider's privacy policies before making healthcare decisions, but would eliminate certain of the concerns related to obtaining quality healthcare as well as the barriers formed with respect to patients' access to care under the Privacy Rule.⁶⁰ Nevertheless, as the Privacy Rule is currently written, the consent requirement deters the necessary collaboration of healthcare organizations and others that are part of the chain of trust and thus impedes the quality of and access to healthcare.

In addition to the consent requirement, the Privacy Rule's minimum necessary standard further amplifies the administrative burdens that Covered Entities will encounter. In particular, the minimum necessary standard breaks the chain of trust because it requires Covered Entities to limit the use or disclosure of, and requests for, PHI to the *minimum amount necessary* to accomplish the intended purpose.⁶¹ In effectuating this goal, Covered Entities will be required to develop and implement policies and procedures appropriate to the Covered Entity's business practices and workforce that reasonably minimize the amount of PHI used,

disclosed, and requested.⁶² Such policies and procedures must identify the individuals or classes of individuals within the Covered Entity who need access to the PHI to perform their duties, the categories or types of PHI needed, and the conditions appropriate to such access.⁶³ Of particular concern with respect to the minimum necessary standard is the inclusion of oral communications within the scope of PHI. Monitoring such communications raises a host of issues from being extremely costly, quite burdensome to implement, and even impossible to administer.⁶⁴

In addition to being an administrative quagmire, the minimum necessary standard will lead to Covered Entities implementing defensive information practices due to the fear of being non-compliant and thus exposed to potential liability from plaintiffs' lawsuits, DHHS sanctions, Department of Justice criminal investigations, and the costs associated with each. As Covered Entities adopt defensive information practices, important medical information will begin to be withheld ultimately leading to an erosion of the chain of trust and a decline in quality healthcare.⁶⁵

Realizing that the Privacy Rules will lead to irrational actions and consequences, the DHHS is attempting to counter many of these concerns via the Proposed Modifications.⁶⁶ Moreover, the National Committee on Vital and Health Statistics (the NCVHS) recently recommended that the DHHS provide guidance and education on the minimum necessary standard to address the increasing concerns about

liability and defensive information practices that may lessen the flow of information and impede care, and that the DHHS issue advisory opinions and publish best practices to assist in alleviating the administrative burdens that Covered Entities will incur when developing policies.⁶⁷

An additional administrative burden that Covered Entities will face is associated with the Privacy Rule's non-pre-emption of more stringent state privacy laws.⁶⁸ Generally, the Privacy Rule constitutes a "floor" from which states may raise the applicable privacy standards.⁶⁹ Additionally, the Privacy Rule does not preempt state provisions that the DHHS Secretary determines are necessary to: (1) prevent fraud and abuse; (2) insure regulations of insurance and health plans; (3) improve the healthcare system; or (4) address controlled substances.⁷⁰ Such an exception for state laws that are more stringent than the Privacy Rule will be difficult to apply with any degree of uniformity as it may subject Covered Entities to a variety of multiple state laws depending upon where the patient is located.⁷¹ Ultimately, this provision could become an administrative nightmare forcing Covered Entities to establish a number of policies that are contingent upon location. Moreover, it is likely that Covered Entities will interpret state statutory provisions differently thus leading to inevitable litigation to reach some uniformity on the issues. The Privacy Rule's "more stringent" exception also will encourage state law makers to expand upon existing privacy protections, which, in turn, will require Covered Entities to bear the legal costs associated with continuously monitoring state

developments in order to modify their privacy practices accordingly.⁷²

B. Private Lawsuits

Significantly, HIPAA does not authorize a private cause of action.⁷³ Nevertheless, non-compliance with the Privacy Rule may become the basis for holding Covered Entities liable under common law actions for breach of confidentiality.⁷⁴ As one federal district court recently noted about the Privacy Rule, "the Standards indicate a strong federal policy to protect the privacy of patient medical records, and they provide guidance to the present case."⁷⁵

Indeed, many state courts have recognized that, even where statutory provisions deny a private cause of action, a statute may set the standard against which a defendant's actions could be measured. In *Doe v. Community Health Plan Kaiser Corp.*⁷⁶, a court examined an allegedly improper disclosure of confidential information by an employee of an HMO. After considering certain statutory provisions that precluded unauthorized disclosures by HMOs and healthcare providers, the court opined that "[w]hile a private cause of action may not be predicated on . . . these statutes, [they] define and impose the scope of the actionable duty of confidentiality which arises between certain healthcare providers . . . and their patients."⁷⁷

Recognizing that the Privacy Rule may become the base standard against which healthcare entities will be measured arguably leads to the drastic result of Covered Entities incurring substantial costs in defend-

ing lawsuits brought by plaintiffs for the most nominal breach of the Privacy Rule. Indeed, the prevailing case law substantially supports a plaintiffs' cause of action for breach of confidence.⁷⁸ For example, in examining whether an unconsented disclosure by a physician to his patient's employer gave rise to a cause of action, the Alabama Supreme Court held that the plaintiff had properly asserted a claim for breach of a confidential relationship.⁷⁹ In *Hammonds v. Aetna Casualty & Surety Co.*, the court, in considering whether a physician may be held liable for breach of a confidential relationship, opined:

The unauthorized revelation of medical secrets, or any confidential communication given in the course of treatment is tortious conduct which may be the basis for an action in damages.⁸⁰

With such a solid foundation existing at common law, it is inevitable that the plaintiffs' bar will become more conversant in the Privacy Rule and the countless ways that a Covered Entity can run afoul of it. As jury verdicts against Covered Entities become prevalent, the use of defensive information tactics by Covered Entities will become ever more necessary.

Business Associates also should be concerned about exposure to liability under the Privacy Rule. While the DHHS Secretary deleted a provision in the proposed privacy regulations that required any Business Associate agreement to explicitly state that individuals were third party beneficiaries to the contract, the Privacy Rule does not prohibit

Continued on page 6

Continued from page 5

individuals from bringing a third party beneficiary claim under common law. Indeed, the DHHS Secretary warned the healthcare industry: "If existing law allows individuals to claim third party beneficiary rights or prohibits them from doing so, [the DHHS] does not intend to affect those rules. Rather, [the DHHS] intend[s] to leave this matter to such other law."⁸¹

Many jurisdictions have adopted the RESTATEMENT (SECOND) OF CONTRACTS view that an intended beneficiary has an enforceable right under a contract.⁸² Indeed, several state courts already have recognized a legal basis for extending liability to a third party receiving confidential health-related information. For example, in *Biddle v. Warren General Hospital*⁸³, the Ohio Supreme Court recognized the existence of a tort where a hospital, at the insistence of its lawyers, forwarded patient registration forms to the law firm prior to obtaining the patients' consents. In holding the law firm liable for the disclosure by the hospital, the court stated:

[A] third party can be held liable for inducing the unauthorized, unprivileged disclosure of nonpublic medical information that a physician or hospital has learned within a physician-patient relationship.⁸⁴

Accordingly, Business Associates should not feel immune from litigation with respect to the Privacy Rule as they may incur substantial costs resulting from third party beneficiary suits brought by aggrieved patients for the improper use or disclosure of

PHI. Due to the potential exposure to liability to both Covered Entities and Business Associates, it ultimately will be advisable, if not necessary, for Covered Entities and Business Associates to protect their respective interests by negotiating indemnification clauses into the Business Associate arrangement.

The Privacy Rule also may serve as a catalyst to increased medical malpractice litigation as Covered Entities will be required to more accurately account for medical records and plaintiffs will be better equipped to exploit some of the new privacy protections for litigation purposes.⁸⁵ In particular, the Privacy Rule gives the patient a "right of access to inspect and obtain a copy of protected health information."⁸⁶ Plaintiffs likely will use their right of access as the first step in assessing whether malpractice has been committed.⁸⁷ Moreover, "an individual has the right to have a covered entity amend protected health information."⁸⁸ Such a right will permit an individual to better portray his or her story and thus reinforce the plaintiff's theory of liability.⁸⁹ This article suggests that, in bestowing substantial rights among patients, the Privacy Rule has established a framework that may foster significant litigation. While the DHHS Secretary may have intended the individual rights to serve as a basis for patient trust in the healthcare system, it is evident from the above discussion that such individual rights eventually may lead to defensive information tactics thus stifling the collaboration among Covered Entities and ultimately breaking the

chain of trust that is necessary for a quality healthcare system.

VI. Conclusion

Protecting privacy and improving quality seem to mandate competing needs. Protecting privacy suggests a need to decrease the flow of patient-related information. By contrast, maximizing the collaboration and sharing of an individual's healthcare information among healthcare providers seem to be key strategies aimed at improving quality of care.⁹⁰ While privacy of confidential information is a critical public health interest, any acceptable privacy regulations should not substantially hinder the collaboration by and among those who are part of the healthcare chain of trust. Due to the administrative costs associated with the Privacy Rule and the increased adversity that may become prevalent between patients and Covered Entities as patients exploit their newly formed rights, it is possible that the Privacy Rule ultimately may serve to undermine HIPAA's goal of an efficient and quality healthcare system.

The Proposed Modifications, if enacted, may serve to reduce several of the Covered Entities' concerns. Nevertheless, this article cautions that as protecting patients' confidences becomes the dominant concern and healthcare entities are distracted from quality of care issues like those debated with respect to the Patients' Bill of Rights, healthcare entities increasingly will engage in defensive information practices. Protecting patient confidences is crucial to establishing patients' trust in the healthcare system as it fosters candid discussions about healthcare symptoms. However, ultimately,

defensive information practices only can lead to the erosion of quality healthcare as those in the healthcare chain of trust will be less likely to collaborate and share necessary medical information. Such a break in the chain of trust is arguably the antithesis of what the Privacy Rule was expected to accomplish.

Endnotes

- ¹ Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1988 (1996).
- ² D'Arcy Guerin Gue, *Transactions and Code Sets: For Geeks Only?*, at www.hipaadvisory.com/action/tcs/geeksonly.htm.
- ³ *Id.*
- ⁴ *Id.*
- ⁵ Nicholas T. Terry, *An eHealth Diptych: The Impact of Privacy Regulation on Medical Error and Malpractice Litigation*, 27 AM. J.L. & MED. 361 (2001).
- ⁶ Standards for Privacy of Individually Identifiable Health Information; 67 Fed. Reg. 14776, 14777 (proposed Mar. 27, 2002) (to be codified at 45 C.F.R. pts. 160 & 164) [hereinafter Proposed Modifications].
- ⁷ "Health plan" is defined as an individual or group plan that provides or pays the cost of medical care (as that term is defined in 42 U.S.C. § 300gg-91(2)(a)). 45 C.F.R. § 160.103 (2001).
- ⁸ "Health care clearinghouse" is defined as a public or private entity that performs either of the following functions:
 - (1) Processes or facilitates the processing of health information received from another entity in a non-standard format or containing

<p>nonstandard data content into standard data elements or a standard transaction.</p> <p>(2) Receives a standard transaction from another entity and processes or facilitates the processing of health information into standard format or nonstandard data content for the receiving entity.</p> <p><i>Id.</i></p> <p>⁹ “Health care provider” is defined as a provider of services (as defined in section 1861(u) of the Social Security Act, 42 U.S.C. § 1395x(u)), a provider of medical or health services (as defined in section 1861(s) of the Social Security Act, 42 U.S.C. § 1395x(s)), and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business.</p> <p><i>Id.</i></p> <p>¹⁰ <i>Id.</i> It is worth noting that even healthcare providers who do not submit HIPAA transactions in electronic standard form are still subject to the Privacy Rule if another entity, such as a billing service or a hospital, transmits standard electronic transactions on behalf of such provider. Standards for Privacy of Individually Identifiable Health Information; 65 Fed. Reg. 82462, 82477 (Dec. 28, 2000) (codified at 45 C.F.R. pt. 160) [hereinafter HIPAA Privacy Rule].</p> <p>¹¹ The following are HIPAA transactions: (1) healthcare claims or equivalent encounter information; (2) health claims attachments; (3) enrollment and disenrollment in a health plan; (4) eligibility for a health plan; (5) healthcare payment and remittance advice; (6) health plan premium payments; (7) first report of injury; (8) health claim status; and</p>	<p>(9) referral certification and authorization. HIPAA, <i>supra</i> note 1, § 262.</p> <p>¹² 42 C.F.R. § 164.501 (2001).</p> <p>¹³ HIPAA Privacy Rule, <i>supra</i> note 10, at 82620.</p> <p>¹⁴ <i>Id.</i> at 82533.</p> <p>¹⁵ <i>Id.</i></p> <p>¹⁶ <i>Id.</i></p> <p>¹⁷ <i>Id.</i></p> <p>¹⁸ 45 C.F.R. § 164.504(e) (2001).</p> <p>¹⁹ The term “business associate” is defined as an entity that:</p> <p>(1) On behalf of a Covered Entity performs or assists in the performance of a function or service that involves the use or disclosure of individually identifiable health information or any other function or activity regulated by the Privacy Rule; or</p> <p>(2) Provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services, where the service involves the disclosure of individually identifiable health information from the Covered Entity or from another business associate of a Covered Entity.</p> <p><i>Id.</i> § 160.103.</p> <p>²⁰ HIPAA Privacy Rule, <i>supra</i> note 10, at 82475.</p> <p>²¹ <i>Id.</i>; The services include legal, actuarial, accounting, consulting, data aggregation, management, accreditation, administrative and financial. 45 C.F.R. § 160.103 (2001).</p> <p>²² HIPAA Privacy Rule, <i>supra</i> note 10, at 82475.</p> <p>²³ 45 C.F.R. § 164.502 (2001).</p> <p>²⁴ <i>Id.</i></p>	<p>²⁵ HIPAA Privacy Rule, <i>supra</i> note 10, at 82476.</p> <p>²⁶ <i>Id.</i></p> <p>²⁷ <i>Id.</i></p> <p>²⁸ 45 C.F.R. § 164.502(e)(1) (2001); HIPAA Privacy Rule, <i>supra</i> note 10, at 82504.</p> <p>²⁹ 45 C.F.R. § 164.504(e) (2001).</p> <p>³⁰ <i>Id.</i> § 164.502(e).</p> <p>³¹ <i>Id.</i> § 164.520.</p> <p>³² <i>Id.</i> § 164.522(a).</p> <p>³³ <i>Id.</i> § 164.522(b).</p> <p>³⁴ <i>Id.</i> § 164.524.</p> <p>³⁵ <i>Id.</i> § 164.526.</p> <p>³⁶ <i>Id.</i> § 164.528.</p> <p>³⁷ <i>Id.</i> § 164.530.</p> <p>³⁸ <i>Id.</i> § 165.520(a)(2); HIPAA Privacy Rule, <i>supra</i> note 10, at 82547.</p> <p>³⁹ 45 C.F.R. § 165.520(a)(2) (2001).</p> <p>⁴⁰ HIPAA Privacy Rule, <i>supra</i> note 10, at 82548.</p> <p>⁴¹ <i>Id.</i> at 82472.</p> <p>⁴² 42 U.S.C. § 1176 (2001); HIPAA Privacy Rule, <i>supra</i> note 10, at 82470.</p> <p>⁴³ 42 U.S.C. § 1177 (2001); HIPAA Privacy Rule, <i>supra</i> note 10, at 82470.</p> <p>⁴⁴ 42 U.S.C. § 1177 (2001).</p> <p>⁴⁵ <i>Id.</i></p> <p>⁴⁶ <i>Id.</i></p> <p>⁴⁷ See 45 C.F.R. § 164.506 (2001).</p> <p>⁴⁸ <i>Id.</i></p> <p>⁴⁹ <i>Id.</i></p> <p>⁵⁰ 45 C.F.R. § 164.508 (2001).</p> <p>⁵¹ <i>Id.</i> § 165.508(b)(4).</p> <p>⁵² <i>Id.</i> § 164.508(c).</p> <p>⁵³ <i>Id.</i> § 164.508(d).</p>	<p>⁵⁴ <i>Id.</i> § 164.508(e).</p> <p>⁵⁵ <i>Id.</i> § 164.508(f).</p> <p>⁵⁶ It is worth noting that the Proposed Modifications attempt to standardize the authorization requirement and eliminate the need for different forms of authorizations for different purposes. See Proposed Modification, <i>supra</i> note 6 at 14797.</p> <p>⁵⁷ 45 C.F.R. § 164.506(a).</p> <p>⁵⁸ Proposed Modifications, <i>supra</i> note 6, at 14780.</p> <p>⁵⁹ <i>Id.</i> at 14783-84.</p> <p>⁶⁰ HHS News, <i>HHS Proposes Changes That Protect Privacy, Access To Care</i>, at www.hhs.gov/news/press/2002pres/20020321a.html.</p> <p>⁶¹ See 42 C.F.R. § 164.502(b) (2001); see also Proposed Modifications, <i>supra</i> note 6, at 14784.</p> <p>⁶² 45 C.F.R. § 164.514(d).</p> <p>⁶³ Proposed Modifications, <i>supra</i> note 6, at 14783-1784.</p> <p>⁶⁴ HIPAA Privacy Rule, <i>supra</i> note 10, at 82620.</p> <p>⁶⁵ Proposed Modifications, <i>supra</i> note 6, at 14786.</p> <p>⁶⁶ For example, DHHS proposes to add a provision at § 164.502(a)(1)(iii) to explicitly permit certain incidental uses and disclosures that occur as a result of an otherwise permitted use or disclosure. <i>Id.</i> at 14785. Such incidental disclosures under the Proposed Modifications would be permitted only to the extent the Covered Entity has applied reasonable safeguards and implemented the minimum necessary standard. <i>Id.</i> Moreover, DHHS proposes to exempt any uses or disclosures for which a Covered Entity has received an authorization under § 165.508. <i>Id.</i> at 14785-14786. The Proposed Modifications also modify</p>
--	--	--	---

Continued on page 8

Continued from page 7

§ 164.514(d)(1) to delete the term “reasonably ensure” in response to concerns that the term connotes an absolute standard and is thus inconsistent with DHHS’ position that the minimum necessary requirements be reasonable and flexible. *Id.* Additionally, DHHS clarified that the Privacy Rule is not intended to impede necessary healthcare practices and communications nor to require that any risk of incidental use or disclosure be eliminated to comply with the minimum necessary standard. Accordingly, DHHS indicated that facility redesigns and expensive computer upgrades are not required. Covered Entities may, however, need to make adjustments to facilities to minimize access or provide additional security such as isolating or locking file cabinets and record rooms and provide passwords for computers maintaining PHI. *Id.* at 14785-14787. Moreover, the DHHS explained that Covered Entities are permitted to develop policies and procedures that allow for appropriate individuals to access entire medical records. *Id.* at 14786.

67 *Id.* at 14786-14787.

68 HIPAA Privacy Rules Update, *The Interplay Between the Privacy Regulations and State Laws - A Possible Cause of Action for Breach of Confidence*, at www.ifebp.org/knowledge/hipaa6.asp.

69 *Id.*

70 45 C.F.R. § 160.204 (2001).

71 45 C.F.R. §§ 160.201-.205 (2001).

72 Terry, *supra* note 5, at 368.

73 McDermott Will & Emery Health Law Update, *Final Health Information Privacy Rules*, Vol. 17, No. 11, p. 9 (Jan. 5, 2001), available at www.mwe.com/news/hlu1711.htm.

74 Richard D. Marks, *Guidelines for Initiating HIPAA System Implementation Projects*, 8 Health Care Policy Report, No. 21, p. 857, Bureau of National Affairs (May 22, 2000).

75 *United States v. Sutherland*, 143 F. Supp. 2d 609, 612 (W.D. Va. 2001).

76 709 N.Y.S.2d 215, 216 (N.Y. App. Div. 2000).

77 *Id.* at 217-18; see also *Lingle v. Lion*, 776 So. 2d 1073, 1076 (Fla. Dist. Ct. App. 2001) (holding a cause of action in negligence per se is created when a penal statute protects a class of persons and violation of a statute, code or ordinance which is designed to protect the public constitutes evidence of negligence).

78 See, e.g., *Berger v. Sonneland*, 26 P.3d 257 (Wash. 2001); *Jeffrey H. v. Imai*, 101 Cal.Rptr.2d 916 (Cal. Ct. App. 2000); *Biddle v. Warren Gen. Hosp.*, 715 N.E.2d 518 (Ohio 1999); *McCormick v. England*, 494 S.E.2d 431 (S.C. Ct. App. 1997).

79 *Horne v. Patton*, 287 So. 2d 824 (Ala. 1973).

80 *Hammonds v. Aetna Cas. & Sur. Co.*, 243 F. Supp. 793, 802 (N.D. Ohio 1965).

81 HIPAA Privacy Rule, *supra* note 10, at 82641.

82 RESTATEMENT (SECOND) OF CONTRACTS, § 302.

83 715 N.E.2d 518 (Oh. Sup. Ct. 1999).

84 *Id.*

85 Terry, *supra* note 5, at 384.

86 45 C.F.R. § 164.524(a)(1) (2001).

87 Terry, *supra* note 5, at 362 (further explaining that, to the extent litigation looms closer, 45 C.F.R.

§ 164.528(1)(ii) allows the provider to deny a request to access “[i]nformation compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding.”).

88 45 C.F.R. § 164.526(a)(1) (2001).

89 Terry, *supra* note 5, at 364.

90 *Id.* at 362.

H M O S & Health Plans Leadership 2001-02

Richard L. Shackelford Chair

King & Spalding
191 Peachtree Street
Atlanta, GA 30303-1763
Phone: (404) 572-4995
Fax: (404) 572-5142
E-Mail:
Rshackelford@kslaw.com

Errol J. King, Vice Chair McGlinchey Stafford, APLLC 9th Floor

One American Place
Baton Rouge, LA 70825
Phone: (225) 383-9000
Fax: (225) 343-3076
E-Mail:
eking@mcglinchey.com

Margit Nahra Vice Chair

Crowell & Moring, LLP
1001 Pennsylvania Ave, NW
Washington, D.C. 20004
Phone: (202) 624-2965
Fax: (202) 628-5116
E-Mail: mnahra@cromor.com

Stuart Silverman Vice Chair and Editor

Office of Inspector General
for the Government
of the District of Columbia
PO Box 30378
Bethesda, MD 20824
Phone: (301) 897-4896
E-Mail: sisilverman@aol.com