THE GOVERNMENT'S NEW PATIENT PRIVACY RULES AND HEALTH CARE FRAUD COMPLIANCE AND ENFORCEMENT: CAN INFORMANTS BLOW THE WHISTLE? CAN PROVIDERS MEET THEIR COMPLIANCE RESPONSIBILITIES? CAN UNCLE SAM INVESTIGATE HEALTH CARE FRAUD?

Shelley R. Slade, Esq.
Vogel & Slade
Washington, D.C.

Introduction

On December 28, 2000, under the authority of the Health Insurance Portability and Accountability Act of 1996 (HIPAA),[1] the Department of Health & Human Services (HHS) issued final Standards for the Privacy of Individually Identifiable Health Information (the "Privacy Rule" or "Rule").[2] HHS's issuance of a comprehensive, complex Privacy Rule naturally has raised questions as to whether patient health records may still be disclosed to, and used by the government in connection with health care fraud enforcement work. The issue is a significant one: patient-specific information is often critical to proving the falsity of health care claims. For example, review of patient charts ordinarily is needed to verify allegations concerning billing for services not provided, billing for medically unnecessary services, duplicate billing, and upcoding.

The answer to the question of whether patient-specific information may still be disclosed and used in the war against health care fraud is an unequivocal "yes" — provided certain requirements are met. This article will focus on those aspects of the Rule with the greatest implications for health care fraud compliance and enforcement, and will provide an overview of the prerequisites to disclosing patient-specific information for different categories of health care fraud reporting, including blowing the whistle; self-reporting; seeking advice from outside counsel; and, disclosure by the government and *qui tam* plaintiffs in False Claims Act[2] proceedings.

Background

HHS's new Privacy Rule, which is accompanied in the Federal Register by more than three hundred pages of background and explanatory preamble,[4] governs the disclosure and use of individually-identifiable health information by those health care providers, clearinghouses, and plans that conduct health care transactions electronically (referred to herein as "covered entities"). For most purposes, the Rule requires health care providers to obtain a patient's authorization or consent before using or disclosing his or her individually-identifiable health information.

State law currently imposes a hodgepodge of requirements relating to the disclosure of health care information.[5] The Rule does not preempt state law that is stricter, covers certain subject matters spelled out in the Rule, or has been exempted from preemption by the Secretary.

HIPAA imposes civil and criminal penalties on offenders.[6] In some instances, the criminal penalties are extremely stiff. For example, if a person violates the Rule with the intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm, a court may impose a fine of up to $250,000, and/or imprisonment of up to 10 years. The Secretary has designated HHS's Office of Civil Rights (OCR) as the HHS office that will be involved in enforcing the regulation, a function that will include, among other things, "providing interpretations and guidance" and "making referrals for criminal prosecution."[7]

The Rule went into effect on April 14, 2001. It requires that most providers bring their practices into conformity with the standards by April 14, 2003, with small providers being given an extra year.[8]

Prior concerns that the Final Rule might undercut health care fraud enforcement efforts have proved to be largely unfounded. In finalizing its rule, HHS carefully balanced the privacy rights of patients against the public's interest in checking health care fraud, and seemingly took great pains to protect the ability of the government to oversee the integrity of government health care programs.

As a general matter, provided that they also comply with applicable state law, health care providers and their associates and employees will remain free to disclose patient records when reporting potential, health care fraud to the appropriate authorities. No patient authorization or consent need be obtained. Likewise, the government will remain free to use its traditional tools to obtain, use, and disclose patient records when investigating and addressing potential health care fraud. While these disclosures may be made without the need to obtain the patient's authorization or consent, as discussed below, there are several hoops through which those making disclosures will have to jump to qualify for the protections established in the new Rule.

Analysis

Disclosures by Whistleblowers

Individuals working for health care providers, clearinghouses and plans, and business associates of these entities, have often disclosed patient records to law enforcement to back up allegations that false claims have been submitted to government health care programs. In many instances, they have done so not as a representative of a health care entity, but rather in their individual capacity as an informant to the government, or a plaintiff under the *qui tam* provisions of the False Claims Act, 31 U.S.C. § 3730(b).[9]

In the preamble to the Privacy Rule, HHS acknowledges that individuals reporting fraud or other violations of law in their private capacity are *not* subject to the Rule. Thus, HHS notes that "[s]ince the HIPAA legislation only applies to covered entities, not their workforces, it is beyond the scope of this rule to directly regulate the whistleblower actions of members of a covered entity's workforce." 65 Fed. Reg. 82,501-02.

As is implicit in the above-quoted statement from the Preamble, however, the Privacy Rule does *indirectly* regulate members of the workforces of covered entities. The Rule does this by requiring covered entities to sanction employees who violate the entity's privacy policies or procedures.[10]

The Rule also *indirectly* regulates business associates of covered entities who perform health care-related functions on behalf of the covered entity. This is accomplished by provisions that require covered entities to enter into contracts or other arrangements with business associates that restrict their ability to use and disclose patient-specific information; if a business associate violates material terms of such an arrangement, and then fail to take reasonable steps to cure the breach, the covered entity must sanction its associate by terminating the arrangement or reporting the violation to the Secretary of HHS.[11]

Accordingly, to fully protect legitimate whistleblowing activity, HHS took additional steps beyond acknowledging in the Preamble that employees are not directly subject to the Rule. Recognizing that entities covered by the Rule might attempt to misuse the sanction requirements in the Rule to penalize whistleblowing that further important public policy objectives, HHS expressly provided in the text of the Rule that employers are not liable under the Rule when employees and "business associates" engage in legitimate, whistleblowing activity,[12] and are not required to impose on employees engaging in such activity the sanctions that otherwise would be required under the Rule.[13]

Disclosures in Support of Good Faith Whistleblowing Don't Violate the Rule

Thus, under 45 C.F.R. 164.502(j), employees and "business associates" of the covered entity may disclose patient records in support of allegations of health care fraud without causing the covered entity to violate the Rule, provided that the disclosure is made either:

(i) to appropriate government and accreditation agencies "for the purpose of" reporting activities that they believe to be either unlawful, in violation of professional or clinical standards, or potentially endangering to one or more patients, workers or the public; or

(ii) to an attorney retained by the employee or business associate for the purpose of determining their "legal options" with regard to the potential misconduct.

To qualify for this safe harbor, the whistleblower must have a "good faith" belief in his or her allegations, a standard which is similar to the standard found in many federal and state statutes that protect whistleblowers from retaliation by their employers through firing, demotion and other types of employment-related actions.

When disclosure is to a government or accreditation agency, it must be to a "health oversight agency or public health authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of the covered entity or to an appropriate health care accreditation organization for the purpose of reporting the allegation of failure to meet professional standards or misconduct by the covered entity."[14]

The term "health oversight agency" is defined in the Rule broadly to include federal, state, local, Indian tribe, and U.S. territory government agencies, and their agents and contractors, that are "authorized by law to oversee the health care system (whether public or private) or government programs in which health information is necessary to determine eligibility or compliance, or to enforce civil rights laws for which health information is relevant."[15]

Importantly, provided that the requirements of this section are met (and assuming their actions comply with state law), employees and business associates of a covered entity may disclose individually-identifiable information under this section without patient authorization or consent, and notwithstanding what the covered entity might have promised patients in its required, "notice of privacy practices for protected health information."[16]

Covered Entities are not Required to Sanction Disclosures that Support Good Faith Whistleblowing

As noted above, activities falling within the purview of this section are also exempt from the provisions in the Privacy Rule that require covered entities to sanction employees for violations of privacy policies and practices. Thus, the Privacy Rule provides that covered entities are not required to sanction:

> "a member of the covered entity's workforce with respect to actions that are covered by and that meet the conditions of § 164.502(j)[the whistleblower provision] . . . ."[17]

continued on page 8

continued from page 7

In her Response to Comments on Section 164.502(j), the Secretary notes that HHS's "purpose in including this provision is to make clear that we are not erecting a new barrier to whistleblowing, and that covered entities may not use this rule as a mechanism for sanctioning workforce members or business associates for whistleblowing activity." 65 Fed. Reg. 82,636. Other federal and state laws affirmatively bar the employer from retaliating against employees for lawful actions taken in order to report fraud to the government.[18]

The protection that the Rule provides whistleblowing "business associates" is less strong than the protection provided to employee informants. This is because, pursuant to the Rule, a covered entity may only disclose patient records to a business associate that agrees not to use or further disclose the information beyond what is permitted or required by the contract or other arrangement entered into between the covered entity and the business associate, or as "required by law."[19] As noted above, covered entities must sanction business associates that don't make reasonable efforts to cure material breaches in these agreements, by terminating dealings, among other things. In contrast to whistleblowing by employees, the Rule nowhere expressly exempts whistleblowing activities *per se* from this sanction requirement.

As a result, business associates who have signed contracts that don't expressly authorize disclosures for "health oversight," and who nonetheless voluntarily disclose patient records to the government, might face claims by covered entities that they are in material breach of their contract and are consequently subject to sanction under the Rule. Business associates would have strong arguments that any contractual provision that bars legitimate whistleblowing is void as it is contrary to public policy, particularly since the Secretary of HHS has indicated her intent that business associates not be sanctioned for such conduct. However, these arguments would not be without litigation risk. Accordingly, business associates who wish to preserve their ability to disclose patient records when reporting potential health care fraud, should insist on contracts that authorize them to disclose such records for "health oversight".

If a business associate does not obtain a contractual authorization to disclose patient records for health oversight, they can still get the evidence that underlies allegations of health care fraud into the hands of law enforcement by doing so pursuant to the contractual authorization to make disclosures "required by law." The business associate may do so by informing government representatives of the nature of the alleged fraud, and then producing the patient records in response to a government subpoena or civil investigative demand seeking the evidence that backs up the allegations. The business associate may also be able to do so pursuant to the federal statutes that require fraud to be pleaded with particularity (Federal Rule of Civil Procedure 9(b)), and that require *qui tam* plaintiffs to provide the Department of Justice with substantially all the material evidence and information that supports their False Claims Act allegations.[20] Elsewhere in the Rule, HHS expressly defines "required by law" to include: (i) the requirements of compulsory process, such as civil investigative demands and OIG subpoenas, and (ii) statutes requiring the production of "information."[21]

Disclosures by Covered Entities for Health Oversight

In certain circumstances, the Privacy Rule authorizes covered entities, without patient consent or authorization, to disclose protected health information for a number of "public policy" purposes set forth in the Rule. These public policy purposes, include, inter alia, "health oversight."[22] The Rule authorizes disclosures to "health oversight agencies" for "health oversight activities", whether the disclosures are self-initiated, voluntary responses to government requests, or compelled responses to government demands.

"Health Oversight" is Defined Broadly to Include Reviews and Investigations of Allegations of False Claims

The Secretary of HHS has indicated quite clearly that the conduct of health care fraud investigations, administrative proceedings, civil litigation and criminal prosecutions are health oversight activities conducted by health oversight agencies, regardless of whether they are performed by a program agency, or an agency traditionally considered to be law enforcement. First, the term "health oversight agency" is defined broadly in the Rule, as explained above. Second, although the Rule provides no specific examples of "health oversight agencies," in the Preamble to the Proposed Rule, HHS indicates that the Department of Justice is a health oversight agency performing health oversight when it conducts health care fraud investigations and proceedings.[23] Third, in the Preamble to the Final Rule, the Secretary explains that agencies such as the FBI, that are traditionally considered "law enforcement," will sometimes function as "health oversight agencies," and that investigation of potential health care fraud by an agency is a "health oversight activity" by a "health oversight agency":

> "For example, traditional law enforcement agencies, such as the Federal Bureau of Investigation, have a significant role in health oversight. . . .
>
> ". . . . where the investigation or activity relates to health care fraud, a covered entity may make a disclosure pursuant to § 164.512(d)(1),

allowing uses and disclosures for health oversight activities."[24]

Fourth, in the text of the Rule itself, HHS defines health oversight activities broadly by specifying only what it does *not* include. Thus, HHS explains that health oversight does not include investigations and other activities in which "the individual is the subject of the investigation or activity and such investigation or activity does not arise out of and is not directly related to: (i) the receipt of health care; (ii) a claim for public benefits related to health; or (iii) Qualification for, or receipt of, public benefits or services when a patient's health is integral to the claim for public benefits or services."[25]

The Rule Supports HHS-OIG's Voluntary Disclosure Program by Authorizing Disclosures in Connection With Self-Initiated Reporting of Health Care Fraud

Significantly, the Rule authorizes disclosures for health oversight without patient consent or authorization even when such disclosures are self-initiated, *i.e.*, unaccompanied by a government request. The Rule's authorization of disclosures in connection with self-initiated reporting of health care fraud buttresses the ability of health care providers and others to make thorough, self-disclosures when they encounter potential health care fraud, actions that are strongly encouraged by current federal policies.[26]

Covered Entities Must Comply with Substantive and Procedural Requirements to Disclose Patient Records for Health Oversight Activities

As with the whistleblowing provision, however, HHS does not provide a blanket permission for disclosures for health oversight. First, the disclosure must be to a health oversight agency, as defined in the rule. The covered entity must verify the identity and authority of the public official to whom disclosure is made.[27] Second, unless the disclosure is required by law, *e.g.*, required by an OIG subpoena or civil investigative demand,[28] the covered entity must make "reasonable efforts" to limit the disclosed information to "the minimum necessary to accomplish the intended purpose."[29] In assessing what is the "minimum amount" of information needed to accomplish the health oversight purpose, a covered entity may rely on a public official's representation that the information requested is the minimum necessary for the stated purpose, but only if "such reliance is reasonable under the circumstances."[30]

Covered Entities Should Consider Avoiding Restrictions on Health Oversight Use in Notices of Privacy Practices

Providers, clearinghouses, and plans that wish to preserve their ability to disclose patient-specific information as part of a voluntary disclosure of potential health care fraud will need to exercise care in drafting their required notices of privacy practices to ensure that their notices to not preclude them from doing so. Covered entities have the option of issuing notices in which they state their intent to restrict their practices to a greater extent than does the Privacy Rule.[31] Once they have done so, however, the Rule requires them to adhere to this stated intent.[32] If covered entities agree in patient notices not to make disclosures for health oversight without patient consent or authorization, they may later conclude that they have ill-advisedly complicated their ability to voluntarily disclose a practice such as upcoding, or billing for services not rendered, that is seen only through an examination of patient-specific information.

Disclosures by Covered Entities to Outside Counsel

When entities covered by the Privacy Rule utilize the services of outside counsel, consultants and auditors in connection with reviewing allegations of health care fraud, they should bear in mind that these outside professionals may fall within the scope of the term "business associate," triggering the contractual and sanction provisions of the Rule.[33] The term "business associate" is defined in the Rule to include, among other things, "a person who" "provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consultation . . . services to or for such covered entity . . . where the provision of the service involves the disclosure of individually identifiable health information from such covered entity . . . or from another business associate of such covered entity . . . to the person."[34]

Attorneys serving as "business associates" of covered entities should note that the Rule will require them to enter into contracts or other arrangements with their clients in which they agree to: (i) "[m]ake available the information required to provide an accounting of disclosures", and (ii) make their "internal practices, books, and records relating to the use and disclosure of protected health information received from, or created or received by the business associate on behalf of, the covered entity available to the Secretary for purposes of determining the covered entity's compliance with this subpart. . . ."[35] The Secretary does agree that "[p]rotected health information obtained by the Secretary [to investigate or review compliance] will not be disclosed by the Secretary, except if necessary for ascertaining or enforcing compliance with the applicable requirements of this part 160 and the applicable standards, requirements and implementation specifications of subpart E of part 164 of this subchapter, or if otherwise required by law."[36] Nonetheless, to minimize the risk of waiver of privilege that might result from application of these provisions, when feasible and advisable under the circumstances, counsel may wish to provide advice based only on redacted health care information that does not identify the individual patient, and consequently is not protected by the Rule. By doing so, counsel can avoid the restrictions of the "business associate" provisions.

continued on page 10

continued from page 9

Government's Access to and Use of Patient-Specific Information in Administrative and Judicial Proceedings

The government may rely on the liberal "health oversight" authorization even when seeking patient records in judicial and administrative proceedings. Subsection 164.512(e) of the Final Rule authorizes covered entities to disclose patient records in judicial and administrative proceedings if certain procedural and substantive requirements are met. In certain circumstances, these requirements are more onerous than the requirements imposed by the "health oversight" subsection, discussed above. For example, pursuant to the judicial and administrative proceedings subsection, disclosures may be made to a party to the proceeding in response to a subpoena from the party or a discovery request only if the covered entity receives "satisfactory assurance" that the party has made reasonable efforts either to notify the individual whose records are to be disclosed, or to secure a protective order.

In the Final Privacy Rule, HHS clarifies that a health oversight agency in litigation may obtain patient-specific information under the more liberal "health oversight" subsection (45 C.F.R. § 164.512(d), without a need to comply with the stricter requirements in the judicial and administrative proceedings provision (45 C.F.R. § 164.512(e)). Thus, clause (2) of subsection 164.512(e) provides as follows:

> "The provisions of this paragraph do not supersede other provisions of this Section that otherwise permit or restrict uses or disclosures of protected health information."

In the Background to this subsection, the Secretary more directly states:

> "We clarify that the provisions of this [judicial and administrative proceedings] paragraph do not supersede or otherwise invalidate other provisions of this rule that permit uses and disclosures of protected health information. For example, the fact that protected health information is the subject of a matter before a court or tribunal does not prevent its disclosure under another provision of the rule, such as §§ 164.512(b), 164.512(d) [health oversight], or 164.512(f), even if a public agency's method of requesting the information is pursuant to an administrative proceeding."[37]

Once a law enforcement or investigatory agency, such as HHS's OIG or the Department of Justice, has obtained individually identifiable health information from a covered entity disclosing the information under the health oversight provision or otherwise, it may use such information for official purposes, including in administrative and judicial proceedings, without being subject to any restrictions imposed by the Privacy Rule. By its terms, the Privacy Rule directly regulates only covered entities, *i.e.*, health care providers, plans and clearinghouses. It does not regulate law enforcement or investigatory agencies.

Disclosures to *Qui Tam* Plaintiffs in Cases in Which The United States has Declined to Intervene

The civil False Claims Act authorizes private *qui tam* plaintiffs who file actions under the Act to litigate their claims on their own if the United States declines to "intervene in," or in other words, formally enter the case.[38] Once the United States has declined to intervene, a *qui tam* plaintiff ordinarily will have to use traditional, judicial discovery tools to obtain documents such as patient records, since the government likely will no longer be investigating the claims. The new rules will require *qui tam* plaintiffs to jump through additional hoops to obtain protected health information in litigation, but these hoops should not prove to be overly burdensome.

Thus, pursuant to the Privacy Rule, a covered entity may always produce protected health information to a *qui tam* plaintiff in response to a court order that expressly calls for production of the information.[39] In addition, covered entities may produce protected information in response to judicial subpoenas and discovery requests from *qui tam* plaintiffs that are unaccompanied by court orders, *provided that* the covered entity receives "satisfactory assurance," a term defined in the Rule, that the party seeking the information has made "reasonable efforts" either (i) "to ensure that the individual who is the subject of the protected health information . . . has been given notice of the request," or (ii) "to secure a qualified protective order that meets the requirements [of the Rule]."[40]

The Rule contains detailed specifications regarding what constitutes "satisfactory assurance" that the party requesting the information has provided notice to the individual. These include a statement and documentation of a good faith attempt to provide notice to the individual as to the nature of the proceeding, and the opportunity to object to disclosure, with either no objection having been made within the time to object, or all objections having been resolved.

Providing "satisfactory assurance" that a qualified protective order has been requested is likely to be a preferable option for *qui tam* plaintiffs in cases involving numerous patient records. To provide satisfactory assurance that a qualified protective order has been requested, the party requesting disclosure need only show that both parties to the dispute have stipulated to an agreement that has been presented to the Court, or the party requesting disclosure has moved the court for an order, and that the agreement or proposed order:

"(A) Prohibits the parties from using or disclosing the protected health information for any purpose other than the litigation or proceeding for which such information was requested; and

"(B) Requires the return to the covered entity or destruction of the protected health information (including all copies made) at the end of the litigation or proceeding."

Significantly, the Rule does not require that the court enter the requested protective order before disclosure may be made.

A covered entity also may disclose protected health information to *qui tam* plaintiffs, in response to lawful process, if the covered entity makes reasonable efforts to notify the individual whose health information is to be disclosed, or to secure a qualified protective order.

Patient Authorizations and "De-Identified" Information

Counsel considering disclosing individually-identifiable health information in connection with the reporting of health care fraud, should bear in mind that there are two viable alternatives to disclosure under the "whistleblower," "required by law," and "health oversight" provisions. The first is to obtain the patient's authorization for the disclosure in conformity with the requirements in 45 C.F.R. § 164.508. If a valid patient authorization is obtained, a covered entity need not worry about meeting the requirements of the other disclosure provisions, such as the requirement that self-initiated disclosures for "health oversight" include no more than the "minimum" information "necessary."

The second option is to redact the patient records to eliminate the individually-identifiable health information. Records that have been redacted in the stringent manner set forth in the Rule[41] will not trigger the protections of the Rule,[42] and consequently will eliminate the need for compliance with the requirements discussed above, including the need to determine what amount of information is the "minimum necessary" for a health oversight purpose. In cases involving a small number of patient records, or a large number of records and a disclosing entity with significant administrative resources available to perform the redacting, it may be best to "de-identify" the health information following the procedures set forth in the Rule, using a key, if appropriate, to link records relating to the same patient.

Conclusion

In sum, HHS's final Rule adequately protects the ability of the health care industry, the taxpayer, and the government to disclose, investigate, and prosecute health care fraud to safeguard the public fisc. While disclosures of unredacted, individually-identifiable information will have to be made in compliance with new federal procedures, the Rule serves only to curb gratuitous disclosures; disclosures in connection with legitimate reporting of potential fraud should not be hindered. State privacy law will need to be consulted as before, since the Rule does not preempt certain state law. In addition, counsel will need to determine whether other federal statutory and case law addressing discrete categories of health information might restrict disclosure.[43] Finally, counsel should ascertain whether HHS's Office of Civil Rights or the courts have interpreted or modified any provisions of the Rule relied upon in making a disclosure.

Shelley R. Slade is a member of Vogel & Slade, LLP, a Washington D.C. law firm that specializes in matters involving health care compliance and allegations of fraud, including matters arising under the federal False Claims Act. In 1998 and 1999, Ms. Slade was the Senior Counsel for Health Care Fraud in the Civil Division of the United States Department of Justice. In that position, she handled health care fraud policy and legislative issues for the Civil Division. From 1990 until 1997, she handled *qui tam* and other False Claims Act cases in the Commercial Litigation Branch of the Department of Justice. She practiced law at Arnold & Porter from 1984 until 1989. She is a graduate of Stanford Law School, and received her bachelor of arts degree *magna cum laude* from Princeton University.

Endnotes

1 *See* P.L. 104-191, Section 262, codified at 42 U.S.C. 1320d-1329d-8.

2 65 Fed. Reg. 82,798 - 82,829 (December 28, 2000).

3 31 U.S.C. § 3729 *et seq.*

4 *See* 65 Fed. Reg. 82,462-82,798.

5 In the preamble to the Rule, the Secretary noted that "[w]hile virtually every state has enacted one or more laws to safeguard privacy, these laws vary significantly from state to state . . . ." 65 Fed. Reg. 82,463.

6 *See* 42 U.S.C. § 1320d-6.

7 65 Fed. Reg. 82,472.

8 45 C.F.R. § 164.534.

9 The False Claims Act, 31 U.S.C. § 3729 et seq., which imposes liability for treble damage and statutory penalties on those who knowingly make false claims for federal funds, permits private persons to file actions on behalf of the United States. The Act requires that private persons who file actions under the Act disclose in writing to the Department of Justice "substantially all material evidence and information the person possesses" in support of the alleged violations of the False Claims Act. 31 U.S.C. § 3730(b)(2). Moreover, courts have held that violations of the False Claims Act must be pled with particularity. *See, e.g., United States ex rel. Stinson v. Blue Cross Blue Shield, Inc.*, 755 F. Supp. 1055(S.D. Ga. 1990).

10 45 C.F.R. § 164.530(e)(1).

11 45 C.F.R. § 164.502(e) at 65 Fed. Reg. 82,806; 45 C.F.R. § 164.504(e) at 65 Fed. Reg. 82,808-09.

12 45 C.F.R. § 164.502(j).

13 45 C.F.R. § 164.530(e)(1).

14 45 C.F.R. § 164.502(j)(1)(ii)(A).

15 45 C.F.R. § 164.501.

16 *See* 45 C.F.R. § 164.502 at 65 Fed. Reg. 82,805-07.

17 *Id.*

18 *See*, e.g., 31 U.S.C. § 3730(h).

19 45 C.F.R. § 164.504(e)(2)(ii)(A) at 65 Fed. Reg. 82,808.

20 31 U.S.C. § 3730(b)(2).

21 45 C.F.R. § 164.501.

22 45 C.F.R. § 164.512(d).

23 *See* 64 Fed. Reg. 59,958 (November 3, 1999).

24 64 Fed. Reg. 82,673.

25 45 C.F.R. § 164.512(d)(2).

26 Encouraging effective compliance programs and the voluntary reporting of health care fraud are critical tenets of the health care fraud enforcement strategy pursued by HHS's Office of Inspector General (OIG). Thus, the

continued on page 12

continued from page 11

"Model Compliance Guidances" issued by OIG have urged health care providers to implement compliance plans that include the voluntary reporting of indicia of fraud to the Department of Justice or HHS OIG. The OIG's Voluntary Disclosure Program is based on the assumption that providers will remain free to report evidence of fraud if they choose, and will not encounter federal rules that prohibit or restrict their ability to expeditiously report fraud to the right authorities.

27 45 C.F.R. § 164.514(h).

28 *See* 45 C.F.R. § 164.502(b)(2)(iv).

29 45 C.F.R. § 164.502(b)(1) at 65 Fed. Reg. 82,805.

30 45 C.F.R. § 164.514(d)(3)(iii)(A).

31 45 C.F.R. § 164.520(b)(2) at 65 Fed. Reg. 82,821.

32 45 C.F.R. § 164.502(i) at 65 Fed. Reg. 82,807.

33 45 C.F.R. § 164.502(e) at 65 Fed. Reg. 82,806; 45 C.F.R. § 164.504(e) at 65 Fed. Reg. 82,808.

34 45 C.F.R. § 164.103.

35 45 C.F.R. § 164.504(e)(2)(ii)(G) and (H).

36 45 C.F.R. § 164.310(c)(3) at 65 Fed. Reg. 82,802.

37 65 Fed. Reg. 82,530.

38 31 U.S.C. § 3730(b)(4)(B).

39 45 C.F.R. § 164.512(e)(1)(i).

40 45 C.F.R. § 164.512(e)(1)(ii).

41 45 C.F.R. § 164.514(a)-(c) at 65 Fed. Reg. 82,818-19.

42 45 C.F.R. § 164.502(d)(2).

43 Other federal statutes imposing restrictions on disclosure of health care information include, but are not limited to, the Clinical Laboratory Improvement Act Amendments, 42 U.S.C. § 263a, the Confidentiality of Substance Abuse Records statute, 42 U.S.C. § 290dd-2, and the Privacy Act, 5 U.S.C. § 552a (relevant for certain federal government health plans and contractors). Certain psychotherapy records are protected under Supreme Court case law.