Department of the Treasury **Internal Revenue Service** **Office of Chief Counsel**

Notice

CC-2004-034

September 10, 2004

Subject: Effect of the Health Insurance Portability and Accountability Act of 1996 Privacy Regulations, 45 C.F.R. parts 160 and 164, on the Service's Information Gathering Activities

Cancel Date: Upon incorporation into CCDM

Purpose

This Notice discusses the effect of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Regulations, 45 C.F.R. parts 160 and 164, when the Service requests protected health information from a taxpayer or third party. Under these regulations, the Service will generally have additional burdens when requesting protected health information from a "covered entity" or a covered entity's business associate. There are three exceptions that allow the Service to obtain protected health information while enforcing the Internal Revenue Code: the consent of the taxpayer, the law enforcement exception, and the administrative and judicial proceedings exception. This Notice discusses the standards for applying these exceptions.

Discussion

I. In General

Congress passed the Health Insurance Portability and Accountability Act of 1996, in part, to provide protection for the privacy interest of healthcare patients. Among the numerous subsections of HIPAA, Title II, Subtitle F addresses the privacy rights of individuals whose healthcare records are maintained or transmitted by "covered entities" (e.g., physicians, healthcare organizations, health insurers, etc.). Subtitle F authorizes the Secretary of Health and Human Services to establish privacy regulations for the protection of healthcare information that identifies an individual.

Pursuant to the authority granted in HIPAA, regulations were promulgated authorizing and/or prohibiting disclosure of certain information. *See* 45 C.F.R. §§ 164.102-164.534 (effective April 14, 2003). The rules have the effect of restricting the Service's

Filing Instructions: Binder

NO: Circulate ___ Distribute X to: All Personnel X Attorneys ___ In: ___

Other ___

Electronic Filename: CC-2004-034 Original signed copy in: CC:FM:PM:P

information gathering authority by imposing civil and criminal penalties on "covered entities" for unauthorized disclosure of "protected health information." The privacy rules may limit access to protected health information when the Service is conducting an examination of a covered entity as the taxpayer (e.g., an examination of a hospital or a qualifying employer-sponsored group health plan), or when the Service needs to examine records maintained by a covered entity which are protected under HIPAA (e.g., attempting to obtain medical records to characterize transfers in an estate tax examination or summoning a doctor's billing records to collect an assessed liability).

The privacy rules do not limit the ability of taxpayers to disclose their own medical records. Instead, the rules only govern "covered entities" and their "business associates." A covered entity is defined as a healthcare clearing house, an insurance plan, and includes most healthcare providers.[1] 45 C.F.R. § 160.103. Business associates generally include all third parties that obtain protected health information while providing services to a covered entity. The definition of business associates includes lawyers, accountants, consultants, and entities hired to handle administrative services (e.g., billing). 45 C.F.R. § 160.103. Covered entities are required to enter into contracts with their business associates that will subject the business associate to the privacy rules. The business associates must assure that their sub-contractors and agents also comply with the rules.

Since the Service is acting pursuant to the provisions of the Internal Revenue Code when it is investigating taxpayers, the Service is neither a covered entity nor a business associate. Thus, the Service is not required to enter into a business associate arrangement or any other confidentiality agreement with a covered entity and/or their agents in order to obtain protected health information. While the privacy rules restrict the ability of a covered entity or business associate to release protected health information to the Service, the rules impose no restrictions on the Service itself. Once the Service obtains protected health information, the privacy rules do not govern the subsequent use of the information obtained (including its use for other taxpayer

[1] The rules only apply to healthcare providers who transmit health information in an electronic form in connection with a transaction covered by 45 C.F.R. §§ 160, 162, and 164. Transactions covered by these regulations are enumerated in 42 U.S.C. § 1320d- 2(a)(2) and include: "(A) Health claims or equivalent encounter information. (B) Health claims attachments. (C) Enrollment and disenrollment in a health plan. (D) Eligibility for a health plan. (E) Healthcare payment and remittance advice. (F) Health plan premium payments. (G) First report of injury. (H) Health claim status. (I) Referral certification and authorization." Furthermore, covered transactions include "other financial and administrative transactions determined appropriate by the Secretary, consistent with the goals of improving the operation of the healthcare system and reducing administrative costs." 42 U.S.C. § 1320d-2(a)(1).

examinations).[2] *See* Exec. Order No. 13181, 65 Fed. Reg. 81321 (Dec. 26, 2000).[3] The Service is, of course, free to negotiate for voluntary production of information through Information Document Requests, compliance with a summons, discovery requests in Tax Court, or any other appropriate method. Voluntary production requests should be structured to ensure that compliance with the request would be consistent with HIPAA's privacy rules. The Service should not enter into any binding privacy agreements for the production of documents when the Service may otherwise compel production.

Protected health information is defined as information, in any form, maintained by a covered entity that can identify the individual and relates to that individual's health, the receipt of healthcare services by the individual, or the past, present, or future payment for the healthcare services provided to the individual. Additionally, documents containing information that would identify the healthcare recipient's relatives, employers, or household members can also qualify as protected information. 45 C.F.R. § 164.514(b). As defined by the rules, protected health information extends far beyond the traditional notions of name, address, medical charts, or notations in a file. It includes recollections of healthcare workers, information that merely provides a connection between an individual and the receipt of healthcare, and information that relates to the individual's health insurance premiums. *See* 45 C.F.R. § 164.501. The definition of protected health information, however, expressly exempts educational records as contained in 20 U.S.C. § 1232(g), as well as employment records held by a covered entity in its role as an employer. To obtain these records, the Service should follow normal information gathering procedures.

Although the privacy rules restrict the release of protected health information, they do not apply to "de-identified" information. 45 C.F.R. § 164.514(a). The privacy rules provide a safe harbor rule for de-identifying otherwise protected health information: i.e., the covered entity can remove all identifiers from the information. 45 C.F.R. § 164.514(b). The privacy rules list eighteen specific identifiers ranging from traditional categories such as name and address to unintuitive categories such as web addresses, biometric identifiers (e.g., finger and voice prints), account numbers, and vehicle identification numbers (e.g., license plates). 45 C.F.R. § 164.514(b)(2)(i)(A) – (R).

In order for a covered entity to satisfy the safe harbor rule, all of the listed identifiers must be removed. *Id*. The information does not satisfy the safe harbor rule if any of

---

[2] The disclosure of such information, however, would be subject to the provisions in I.R.C. § 6103.

[3] The Executive Order specifically states that HIPAA regulations "do not apply to other organizations and individuals that gain access to protected health information, including Federal officials who gain access to health records during health oversight activities." It then imposes restrictions on Government agencies that obtain protected health information through their health oversight activities. The Service's tax examinations are not health oversight activities as defined in the Executive Order.

these eighteen identifiers remain. Accordingly, even though the Service may not be able to identify an individual from the specific information provided by the covered entity, if there is one listed identifier in the information received, the information will not satisfy the safe harbor rule. For example, assume the Service is auditing a health insurance company that qualifies as a covered entity. The Service requests transaction details showing all insurance claims that were actually paid. The furnished report identifies individual transactions using unique account numbers assigned by the insurance company. The report does not contain any other listed identifier. Since an account number is an identifier listed in section 164.514(b)(2)(i)(J), this report will not satisfy the safe harbor rule even though the Service has no practical way of identifying the individuals otherwise associated with those unique account numbers.

In addition to the safe harbor rule, the privacy rules permit disclosure that is based upon an expert's written certification that "the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify who is a subject of the information." 45 C.F.R. § 164.514(b)(1). The expert must have "appropriate knowledge of and experience with generally accepted statistical and scientific principals and methods for rendering information not individually identifiable." *Id.*

If information is protected health information, the privacy rules authorize release only where (1) the subject of the protected health information expressly consents to its release, or (2) the release is expressly permitted without consent under another provision of the privacy rules. Although the privacy rules provide several bases for nonconsensual disclosure, the two most relevant to the Service's information gathering procedures are the Law Enforcement and the Judicial and Administrative Procedures exceptions. *See* 45 C.F.R. § 164.512.

II. Obtaining Taxpayer's Authorization for Release of Protected Health Information

HIPAA authorizes a covered entity to release protected health information with the consent of the subject of the protected information. 45 C.F.R. § 164.508. When investigating covered entities or their business associates, the consent would have to be obtained from each person for which protected health information is sought. For example, if the Service sought a doctor's billing records as part of an examination of the doctor, the consent would have to be obtained from each patient identified in the records. In this situation, consent will generally be impracticable.

When the taxpayer is the subject of the protected health information (e.g., challenging the taxpayer's characterization of a jury award in a medical malpractice case), there may be advantages to pursuing consent. First, obtaining a consent may increase a reluctant covered entity's willingness to produce information without a summons enforcement proceeding. Second, if the protected individual refuses to sign a voluntary release, the individual's explanation of the refusal may put the Service in a better position to evaluate the need for compulsory production proceedings. Third, if the

taxpayer under audit refuses consent, the taxpayer retains the burden of proof under I.R.C. § 7491(a).

A valid authorization to release protected health information must contain the following elements: (1) a specific and meaningful description of the information to be disclosed; (2) the name or specific identification of the person authorized to make the disclosure; (3) the name or specific identification of the persons to whom the disclosure may be made; (4) a description of the purpose of the requested use or disclosure of the information; (5) an expiration date; and (6) the signature of the consenting individual and date (if signed by a representative, a description of the representative's authority to act). 45 C.F.R. 164.508(c)(1)(i)-(vi). In addition, the release authorization must contain statements adequate to notify the individual of (1) the individual's right to revoke the authorization; (2) the exceptions to the right to revoke the authorization; (3) a description of how the individual may revoke the authorization; and (4) a statement that the information may be redisclosed and is no longer protected. 45 C.F.R. 164.508(c)(2).

III. Law Enforcement Exception

Permissible law enforcement disclosures include those that are (1) required by law; (2) required under a court order, a court-ordered warrant, or subpoena or summons issued by a judicial officer; (3) required by a grand jury subpoena; or (4) required by an administrative summons or civil investigative demand (CID). 45 C.F.R. §§ 164.512(f)(1)(i), 164.512(f)(1)(ii)(A), 164.512(f)(1)(ii)(B), 164.512(f)(1)(ii)(C). Administrative summonses issued under section 7602(a)(2), grand jury subpoenas, and judicially authorized search warrants all qualify under the law enforcement exception and may be utilized when appropriate.

While the Service maintains the ability to summon information under the privacy rules, the rules impose additional requirements on the Service for administrative summonses. Protected health information sought pursuant to a summons must satisfy an additional three-pronged test: (1) the information sought must be "relevant and material" to a "legitimate law enforcement inquiry"; (2) the request must be "specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought"; *and* (3) "de-identified information could not reasonably be used." 45 C.F.R. § 164.512(f)(1)(ii)(C). These privacy rules are in addition to any statutory or judicial requirement for issuing a summons. To satisfy the requirements of the three-pronged test, the Service should supplement any summons for protected health information with a statement that the three prongs have been met. Under the privacy rules, a covered entity may reasonably rely on such statements and produce summoned information. 45 C.F.R. § 164.514(h)(2).[4] The Service should also

[4] The privacy rules place additional obligations on the Service by preventing a covered entity from releasing protected information pursuant to a summons unless the three prong test discussed above is satisfied. It is unlikely a court would enforce a summons when production would violate the privacy rules. Thus, as a practical matter the Service may have the burden of proving the three prongs contained in 45 C.F.R.

incorporate these standards when drafting affidavits to accompany suit requests to enforce summonses.[5]

IV. Information Document Requests and Other Informal Information Requests

As discussed above, the privacy rules permit production pursuant to a civil investigative demand. 54 C.F.R. § 164.512(f)(1)(ii)(C). A CID is a term of art that refers to a demand for information that is enforceable in a court of law. *See* 65 Fed. Reg. at 82531 (Dec. 28, 2000) (noting that the CID requirement was changed in the final regulation to comply with the definition of "required by law" currently contained in 45 C.F.R. § 164.501). Although the Service has statutory authority to issue an IDR under sections 7601 and 7602(a)(1), an IDR does not qualify as a CID because the Service does not have authority to enforce it. Accordingly, an IDR or other informal request for information does not satisfy any of the exceptions to the privacy rules' general bar against disclosing protected information, and it would be a HIPAA violation for a covered entity to produce protected health information pursuant to one.
This does not mean, however, that the Service cannot use an IDR when investigating covered entities. As discussed above, the privacy rules only prevent production of protected health information. The Service often uses an IDR as a tool to identify bodies of information in the taxpayer's possession that may be relevant to the audit. The Service then refines its requests through subsequent IDRs. To the extent the Service uses an IDR or other informal request to identify a body of information and does not intend to receive actual protected health information, the privacy rules have no bearing. Furthermore, if the Service only desires unprotected information (e.g., information that does not identify the recipient of healthcare services, de-identified information, or information that is maintained by a covered entity as an employer), the privacy rules impose no limitations.

If the Service is uncertain as to what information the covered entity has in its possession, it can avoid potential conflicts with the privacy rules by inserting the following language in an IDR issued to a covered entity:

> To the extent information that is responsive to this request is protected health information as defined in 45 C.F.R. § 164.501, the information should be de-identified (as provided for in 45 C.F.R. § 164.514) prior to providing it to the IRS.

---

§ 164.512(f)(1)(ii)(C) are satisfied whenever a summoned party refuses to produce protected health information.

[5] Although sections 7602(c) and 7609 generally require notice to the taxpayer when the Service is contacting third parties, both sections contain important exceptions. For example, section 7602(c) exempts contacts made pursuant to a criminal investigation. Section 7609(c)(2)(D) exempts collection summonses. The privacy rules, however, generally entitle an individual to obtain an accounting of protected information released by the covered entity. 45 C.F.R. § 164.528(a). The Service can require a covered entity to suspend any notification for a specified period if disclosure would impede its case development. 45 C.F.R. § 164.528(a)(2)(i).

> When providing de-identified information, include a list of the categories of information that you have redacted. If you are unable to de-identify the information, provide a general description of the information you are not producing including [the Service employee should indicate here what information the Service requires to evaluate the usefulness of the information and/or the propriety of the assertion that the information can not be redacted].

If the Service determines that it needs protected health information after evaluating the taxpayer's response to the IDR, it should then issue a summons for the information. There is no legal impediment to the Service issuing a summons concurrent with an IDR. If the Service is requesting information that it knows qualifies as protected information under the privacy rules, or if the covered entity has stated it is willing to produce the information but only if the request is accompanied with a summons, the Service may attach a summons for the protected information to its IDR, thus satisfying HIPAA's law enforcement exception.

V. Administrative and Judicial Proceeding Exception

The drafters of the privacy rules concluded that the current system governing disclosures and uses of medical records in the course of litigation, as exemplified by the Federal Rules of Civil Procedure, "does not provide sufficient protection for protected health information." Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82596 (Dec. 28, 2000) (codified at 45 C.F.R. pt 160, 164). Accordingly, the privacy rules contain additional requirements for disclosures in administrative and judicial proceedings. 45 C.F.R. § 164.512(e). An order from a court or an administrative tribunal permits a covered entity to disclose protected health information in that proceeding. In the absence of such an order, covered entities may disclose protected health information in response to a discovery request under the court/tribunal's discovery rules only after one of the following two conditions have been met: (1) the covered entity receives "satisfactory assurance" from the party seeking the information that reasonable efforts have been made to give notice to the individual who is the subject of the protected health information,[6] 45 C.F.R. § 164.512(e)(1)(ii)(A); *or* (2) the covered entity receives satisfactory assurance from the party seeking the information that the parties to the litigation either have entered into a qualified protective order, or that the party seeking the information has requested a qualified protective order from the court, 45 C.F.R. §§ 164.512(e)(1)(ii)(B) and (e)(1)(iv) . For

[6] Whether or not the Service will be able to notify the individual who is the subject of the protected health information will depend on the nature of the case. For example, when investigating a taxpayer's characterization of a jury award from a personal injury, the subject of the information will be the taxpayer under examination and notice will be possible. If the Service is examining a hospital's calculation of discounts it gave for health services under contracts with insurance providers, the hospital's patients will be the subjects of the health information. In such a case, the Service will generally not have the patients' identities and thus would be unable to notify them prior to obtaining the information.

the purpose of the notice provision, satisfactory assurance is defined as a proof of a good faith attempt to provide sufficient written notice of the proceeding to the subject of the protected health information that would allow him to raise an objection to the court, and that no such objection was filed. 45 C.F.R. § 164.512(e)(1)(iii). For the purpose of the qualified protective order provisions, satisfactory assurance is defined as a proof that either the requesting party requested a protected order from the court, or that both parties have agreed to a qualified protective order that has been submitted to the court. 45 C.F.R. § 164.512(e)(1)(iii).

A qualified protective order is defined as either a protective order issued by the court, or a stipulation entered into by both parties. 45 C.F.R. § 164.512(e)(1)(v). It must prohibit the parties from using the information for any purpose other than the litigation or proceeding for which the information was requested.[7] 45 C.F.R. § 164.512(e)(1)(v)(A). The protective order must also require that all protected health information either be returned to the covered entity at the end of the litigation or proceeding or be destroyed. 45 C.F.R. § 164.512(e)(1)(v)(B).

If a covered entity is otherwise permitted to make the disclosure, a request that arises in a litigation context does not convert the request to the stricter privacy rules governing administrative or judicial proceedings. 65 Fed. Reg. 82530 (Dec. 28, 2000). Thus, if a protected person entered into a consent which is still valid at the time of the discovery request in a court proceeding, a covered entity can rely on the earlier consent. Furthermore, if the Service has an enforceable summons outstanding once the case is docketed (i.e., if the summons was issued before the case was docketed, but the Service has not yet moved to enforce it), it may obtain the information under the privacy rules' exception for administrative summonses without satisfying the rules' exception for judicial proceedings. Finally, if the information was obtained in the audit prior to initiating a court proceeding, the Service will not be required to satisfy the HIPAA privacy rules before using the information in the court proceeding.

VI. Minimum Necessary Standard

Once the Service has met one of the standards which permit disclosure of protected health information, the privacy rules impose on the covered entity an obligation to produce only the minimal amount of information necessary for the qualifying purpose. 45 C.F.R. § 164.514(d)(3)(ii).

The HIPAA privacy rules permit a covered entity to reasonably rely on the Service's statement that a requested disclosure is the minimum necessary for its stated purpose. *Id.* at (d)(3)(iii). Accordingly, the Service should accompany any request for protected health information with a written statement that the requested information is the

[7] For the requirements for a protective order in the Tax Court, consult section 7461, the Tax Court's Rules and the cases issued under section 7461. Chief Counsel has historically resisted efforts to seal Tax Court records. See CCDM 35.4.6.5 (7). Accordingly, any proposed agreement to enter into a protective order must be approved by the Associate Chief Counsel (Procedure & Administration).

minimum necessary to carry out the intended purpose. When issuing a summons, the Service should incorporate the statement at the beginning of the description of summoned records.

Although the HIPAA privacy rules permit the covered entity to disclose the requested information, there is no obligation on the covered entity to do so. The privacy rules do not contain an independent compulsory production mechanism to enforce production. Therefore, when the Service is unable to negotiate voluntarily production with a covered entity pursuant to the Service's summons, the Service must seek enforcement.

Conclusion

HIPAA permits a covered entity to provide protected health information to the Service in several situations. For a basic overview of the standards for each permitted production, see Figure 1.

The Service will be able to obtain protected health information without restriction to the extent the recipient of the healthcare services consents in a valid release authorization.

The Service will generally be required to show the following to obtain protected health information from a covered entity pursuant to a summons in a non-docketed case: (1) the information is relevant and material to a legitimate law enforcement inquiry; (2) the request is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought; and (3) "de-identified" information could not reasonably be used.

In order to obtain protected health information from a covered entity in a docketed case, the Service will need to satisfy one of these three criteria if it either does not already possess the information, or if it can not otherwise obtain the information under another exception: (1) obtain a court order; (2) reasonably attempt to

Method of Information Request	Standard Required by HIPAA
Consent of the taxpayer	Consent must contain: (1) Description of the information (2) Person authorized to make the disclosure (3) Persons to whom the disclosure may be made (4) The use of the information (5) An expiration date (6) The signature of the consenting individual and date 45 C.F.R. 164.508(c)(2)
I.R.S. summons pursuant to section 7602(a)(2)	(1) Relevant and material (2) Specific and limited in scope (3) De-identified information will not work 45 C.F.R. § 164.512(f)(1)(ii)(C)
Request for a court order for production of the documents pursuant to a court's discovery rules	Comply with standards set by court
Request for information pursuant to a court's discovery rules, but without a request for a court order requiring production	(1) Attempt to notify the individual who is the subject of the protected health information *or* (2) Enter a qualified protective order with opposing party *or* seek a qualified protective order from the court 45 C.F.R. § 164.512(e)(1)

FIGURE 1

notify the protected individual that it is seeking the information; or (3) enter into a qualified protective order with the taxpayer involved in the litigation or request a protective order from the court.

Due to the lack of established guidance in this area, all referral letters seeking to enforce a summons to obtain protected health information from a covered entity must be forwarded for pre-review by the Chief, Branch 3, Collection, Bankruptcy & Summonses Division, Associate Chief Counsel (Procedure & Administration).

If you have any questions regarding this notice, please contact Joseph W. Clark, CC:PA:CBS:B03 at (202) 622-3630.

/s/
Deborah A. Butler
Associate Chief Counsel
(Procedure & Administration)