North Dakota Law Review

Volume 79 | Number 1 Article 3

2003

HIPAA Requirements for Lawyers - Business Associate Contracts

Gerald E. DeLoss

HIPAA REQUIREMENTS FOR LAWYERS — BUSINESS ASSOCIATE CONTRACTS*

GERALD E. DELOSS**

I. INTRODUCTION

New regulations will soon be imposed upon the health care industry requiring lawyers to review and implement policies, and enter into contracts, with clients who produce or utilize health-related information. Under HIPAA, the Health Insurance Portability and Accountability Act,[1] regulations have been promulgated that require health care providers, plans, and clearinghouses to enter into specialized contracts with third parties known as "business associates."[2] Lawyers are included under the definition of business associates.[3]

Providers, plans, and clearinghouses covered under the regulations will be entering into contracts governing their relationships with business associates.[4] Due to the special nature of the attorney-client relationship, lawyers should be proactive and take the necessary steps to ensure that their relationships with health care entities comply with the law. Thus, lawyers should begin drafting business associate contracts on behalf of these clients.

Lawyers must comply with the contracts or they will place their clients in a position of violating the regulations.[5] A lawyer's failure to comply may result in penalties for the client, not the lawyer.[6] Further, some of the contractual terms required under the regulations may jeopardize the attorney-client privilege or the work product doctrine.[7]

Part II of this article will discuss the background and essential elements of the HIPAA regulations. Part III will discuss the requirements for

---

* A portion of this article was first published in the November 2002 issue of *South Carolina Lawyer* and has been reprinted with permission from the South Carolina Bar.

** Attorney, Barnwell Whaley Patterson & Helms, LLC, Charleston, South Carolina; J.D. with Distinction, University of North Dakota School of Law, 1994. Mr. DeLoss formerly served as law clerk to the Honorable Dale V. Sandstrom of the North Dakota Supreme Court and is licensed to practice law in North Dakota, Minnesota, Maine, and South Carolina.

1. Health Insurance Portability and Accountability Act, Pub. L. No. 104-191, § 1, 110 Stat. 1936, 1936 (1996).
2. Administrative Data Standards and Related Requirements, 45 C.F.R. Pts. 160, 164 (2002).
3. *Id.* § 160.103(ii).
4. *Id.* § 164.502(e)(2).
5. *Id.* § 164.504(e)(1)(ii).
6. *Id.*
7. *Id.* § 164.504(e)(2)(ii)(H).

business associate contracts. Finally, Part IV will discuss the unique issues that arise in the attorney-client relationship.

II. HIPAA

Congress enacted HIPAA in 1996.[8] Under HIPAA, Congress mandated the establishment of standards for the privacy and security of individually identifiable health information.[9] The law gave Congress until August 21, 1999, to pass comprehensive health privacy legislation.[10] When Congress did not enact such legislation, HIPAA required the Secretary of the Department of Health and Human Services (DHHS) to draft such protections by regulation.[11]

In November 1999, the DHHS published proposed regulations to provide new rights and protections against the misuse or disclosure of health information.[12] The regulations took effect on April 14, 2001.[13] The regulations, set forth at 45 C.F.R. Pts. 160 and 164, are entitled "Standards for Privacy of Individually Identifiable Health Information" (Privacy Rule).[14] This rule gives patients more control over how their personal health information is used.[15] The Privacy Rule also mandates that health care providers, health care clearinghouses, and health plans protect health information.[16] The compliance date for health care providers, health plans other than small health plans, and health care clearinghouses is April 14, 2003.[17] The compliance date for small health plans is April 14, 2004.[18]

On March 27, 2002, the Bush Administration issued proposed amendments to the Privacy Rule in response to complaints from the industry.[19] The final version of the Privacy Rule was issued on August 14, 2002, roughly eight months prior to the compliance date for most entities—April

---

8. Health Insurance Portability and Accountability Act, Pub. L. No. 104-191, § 1, 110 Stat. 1936, 1936 (1996).

9. *Id.*

10. *Id.* § 264(c)(1).

11. *Id.*

12. Standards for Privacy of Individually Identifiable Health Information, 64 Fed. Reg. 59,918, 59,918 (Nov. 3, 1999).

13. Standards for Privacy of Individually Identifiable Health Information, 66 Fed. Reg. 12,434, 12,434 (Feb. 26, 2001).

14. *Id.*

15. *Id.*

16. *Id.*

17. *Id.*; Administrative Data Standards and Related Requirements, 45 C.F.R. § 164.534 (2002).

18. 45 C.F.R. § 164.534; 66 Fed. Reg. at 12,434.

19. Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. 14,776, 14,778 (Mar. 27, 2002).

14, 2003.[20] Under the final Privacy Rule, the requirements relating to existing contracts between providers, health plans other than small health plans, clearinghouses, and their agents have been postponed until April 14, 2004.[21]

A. GENERAL REQUIREMENTS

The Privacy Rule governs the use or disclosure of protected health information (PHI) by a covered entity.[22] PHI is information that may identify an individual and relates to the past, present, or future physical or mental health conditions of that individual; the provision of health care to that individual; or the past, present, or future payment for such health care.[23] A "covered entity" includes a health care provider, a health plan, and a health care clearinghouse.[24]

Under the Privacy Rule, a covered entity may only use or disclose PHI in certain situations. A covered entity may use or disclose PHI to an individual who is the subject of the PHI[25] in order to carry out treatment, payment, or health care operations.[26] A covered entity may also use or disclose PHI under an allowed exception in the Privacy Rule,[27] pursuant to a valid "authorization,"[28] or where the PHI has been "de-identified."[29]

In addition, when using or disclosing PHI, a covered entity must make reasonable efforts to limit the use or disclosure to the "minimum necessary" PHI to accomplish the intended purpose.[30] The minimum necessary requirement is not imposed in situations involving the treatment of the individual, when disclosing the PHI to the individual, or when using or disclosing the PHI pursuant to an authorization.[31] The Privacy Rule also requires covered entities to take steps to implement policies that notify individuals of their rights,[32] to implement policies that provide an accounting of

---

20. 66 Fed. Reg. at 12,434; 67 Fed. Reg. at 14,778.

21. Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. 53,182, 53,273 (Aug. 14, 2002).

22. 45 C.F.R. § 164.501.

23. *Id.*

24. *Id.* § 160.103.

25. *Id.* § 164.502(a)(1)(i).

26. *Id.* §§ 164.502(a)(1)(i), 164.506.

27. *Id.* § 164.502(a)(1)(iii), (vi).

28. *Id.* § 164.502(a)(1)(iv).

29. *Id.* De-identified PHI is "[h]ealth information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual." *Id.* § 164.514(a).

30. *Id.* § 164.502(b).

31. *Id.* § 164.502(b)(2)(i)-(iv).

32. *Id.* § 164.520(a)(1).

disclosures to individuals,[33] and to train employees on the HIPAA protections.[34]

B. PENALTIES FOR FAILURE TO COMPLY

A covered entity's failure to comply with the Privacy Rule's requirements may result in civil and criminal penalties. The DHHS may impose penalties of up to $100 per violation, for a maximum of $25,000 per person, per year.[35] In addition, fines of up to $50,000, one year in jail, or both may be imposed.[36] If the covered entity's actions were committed under false pretenses, a fine of up to $100,000, imprisonment of up to five years, or both may be imposed.[37] Finally, if the misconduct occurred with the intent to sell, transfer, or use for commercial advantage, personal gain, or malicious harm, a fine of up to $250,000, imprisonment up to ten years, or both may be imposed upon the violator.[38]

C. BUSINESS ASSOCIATES

The Privacy Rule directly covers health care providers, plans, and clearinghouses.[39] However, the Rule indirectly governs certain third parties pursuant to covered entities' contracts with the third parties.[40] The third parties, termed "business associates," are bound to numerous contractual restrictions that must be imposed under the Privacy Rule.[41]

A business associate is defined rather broadly. A business associate means a person, other than a member of the covered entity's workforce, who performs or assists in the performance of a function or activity involving the use or disclosure of individually identifiable health information,[42] including:

> (A) . . . claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing; or
>
> (B) Any other function or activity regulated by [the Privacy Rule]; or

---

33. *Id.* § 164.528(a)(1).
34. *Id.* § 164.530(b)(1).
35. 42 U.S.C. § 1320d-5(a)(1) (2000).
36. *Id.* § 1320d-6(b)(1).
37. *Id.* § 1320d-6(b)(2).
38. *Id.* § 1320d-6(b)(3).
39. Administrative Data Standards and Related Requirements, 45 C.F.R. § 160.103 (2002).
40. *Id.* § 164.504(e)(2)(ii).
41. *Id.*
42. *Id.* § 160.103.

> (ii) Provides . . . *legal*, actuarial, accounting, consulting, data aggregation, . . . management, administrative, accreditation, or financial services to or for a covered entity, . . . where the provision of the service involves the disclosure of individually identifiable health information.[43]

Lawyers may be business associates if their services involve the use or disclosure of health information.[44] Lawyers that fall under the definition must follow the restrictions and requirements imposed upon business associates.[45]

Prior to disclosing PHI to a business associate, a covered entity must obtain "satisfactory assurances" that the business associate will appropriately safeguard the PHI.[46] Further, the covered entity and the business associate must enter into a written contract or other arrangement.[47] The contract or other arrangement must contain the terms set forth under the Privacy Rule, as described in detail below.[48]

If the business associate fails to comply with the contractual restrictions, the covered entity may be subject to civil and criminal sanctions by the DHHS.[49] If the covered entity knows of a violation by the business associate, it must take steps to cure the breach.[50] If a cure is not possible, the covered entity must terminate the business associate's contract.[51] If termination is not feasible or possible, the covered entity must report the problem to the DHHS.[52]

If covered entities fail to take appropriate action, they will be in violation of the Privacy Rule and subject to the penalties outlined above.[53] Because the Privacy Rule does not directly govern business associates, they are not subject to the penalties or sanctions that may be imposed on covered entities. However, the Rule does not prohibit covered entities from including a contractual penalty for a breach by business associates.[54]

---

43. *Id.* § 160.103(i)(A)-(ii) (emphasis added).
44. *Id.*
45. *Id.* § 164.504(e)(2)(ii).
46. *Id.* § 164.502(e)(1).
47. *Id.* § 164.502(e)(2).
48. *Id.* § 164.504(e)(2)(ii).
49. *Id.* § 164.504(e)(1)(ii); 42 U.S.C. §§ 1320d-5 to 1320d-6 (2000).
50. Administrative Data Standards and Related Requirements, 45 C.F.R. § 164.504(e)(1)(ii) (2002).
51. *Id.*
52. *Id.* § 164.504(e)(1)(ii)(B).
53. *Id.* § 164.504(e).
54. *Id.*

III. BUSINESS ASSOCIATE CONTRACTS

The Privacy Rule requirements for business associate contracts are divided into restrictions for relationships between public or governmental business associates and covered entities,[55] and non-public business associates and covered entities.[56]

A. NON-PUBLIC OR NON-GOVERNMENTAL PARTIES

If either party is non-public, then the Privacy Rule imposes the following general requirements for contracts between most covered entities and business associates. First, the contract must establish the permitted and required uses and disclosures by the business associate, which must not violate the Privacy Rule.[57] Next, the contract must require the business associate to impose appropriate safeguards to prevent use or disclosure of PHI except as provided under the contract.[58] The contract must also require the business associate to report any use or disclosure of PHI in violation of the contract.[59] The covered entity must ensure, under the contract, that the business associate's agents, including subcontractors to whom the business associate provides PHI that was received from the covered entity, also agree to the same restrictions and conditions that apply to the business associate under the contract.[60]

In addition, the contract generally must require the business associate to make PHI available to the individual and the DHHS.[61] However, the regulations do not require a business associate to provide individuals access to their PHI in situations involving PHI compiled in "reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding."[62] Similarly, the contract generally must provide that the business associate will make the PHI available for amendment and will incorporate any amendments into the PHI.[63] Again, the regulations do not require a business associate to make amendments or incorporate amendments into PHI in situations where access would not be permitted, such as when the PHI is compiled for use in a civil, criminal, or administrative proceeding.[64]

---

55. *Id.* § 164.504(e)(3).
56. *Id.* § 164.504(e)(2).
57. *Id.* § 164.504(e)(2)(ii)(A).
58. *Id.* § 164.504(e)(2)(ii)(B).
59. *Id.* § 164.504(e)(2)(ii)(C).
60. *Id.* § 164.504(e)(2)(ii)(D).
61. *Id.* § 164.504(e)(2)(ii)(E).
62. *Id.* § 164.524(a)(1)(ii).
63. *Id.* § 164.504(e)(2)(ii)(F).
64. *Id.* §§ 164.524(a)(1)(ii), 164.526(a)(2)(iii), 164.528.

Further, the contract must provide that the business associate make the PHI available to the covered entity in order to provide an accounting of disclosures.[65] The accounting requirement does not make an exception for PHI compiled for use in a legal proceeding.[66] Accordingly, lawyers may need to produce PHI to covered entity clients to prepare an accounting of disclosures. However, the Privacy Rule does exclude health care operations from those disclosures that must be set forth in an accounting.[67] Conducting or arranging for legal services is considered a health care operation.[68] In addition, lawyers would have to allow an individual access to PHI that was not compiled for an action or proceeding.[69]

The business associate contract must require the business associate to make its "internal practices, books, and records relating to the use and disclosure of" PHI available to the DHHS in order to determine compliance.[70] The contract must provide that upon the termination of the contract, the business associate either return or destroy all PHI, if feasible, or if not feasible, to extend the protections over the PHI and "limit further uses and disclosures."[71] Finally, the contract must allow the covered entity to terminate the contract if it determines that the business associate has violated a material contract term.[72]

In addition, the covered entity may permit the business associate to use PHI for management and administration if it is for proper management and administration or to carry out legal responsibilities.[73] Further, the covered entity may permit the business associate to disclose PHI for management and administration if the following requirements are met:

> (A) The disclosure is required by law; or
>
> (B)(1) The business associate obtains reasonable assurances from the person to whom the information is disclosed that [the PHI] will be held confidentially and used or further disclosed only as required by law or for the purpose for which it was disclosed to the person; and

65. *Id.* § 164.504(e)(2)(ii)(G).
66. *Id.* § 164.528.
67. *Id.* § 164.528(A)(1)(i)
68. *Id.* § 164.501.
69. *Id.* § 164.528.
70. *Id.* § 164.504(e)(2)(ii)(H).
71. *Id.* § 164.504(e)(2)(ii)(I).
72. *Id.* § 164.504(e)(2)(iii).
73. *Id.* § 164.504(e)(4)(i).

(2) The person notifies the business associate of any instances of which it is aware in which the confidentiality of the information has been breached.[74]

The business associate contract places serious constraints upon the business associate. As a result, several unique issues arise in the context of a business associate contract between a covered entity and a lawyer. These issues will be discussed in Part IV.

B. PUBLIC OR GOVERNMENTAL PARTIES

Alternatives to a written contract are available if both the covered entity and the business associate are public or governmental entities. Under the Privacy Rule, governmental parties may enter into a memorandum of understanding that contains the terms and conditions typically set forth in a business associate contract.[75] Parties may also comply with the Privacy Rule's restrictions and protections if other laws, including their own regulations, accomplish the objectives of the Rule.[76]

C. MODEL BUSINESS ASSOCIATE CONTRACT

In response to concerns raised by covered entities and business associates, the DHHS issued a model business associate contract (model contract) under the proposed amendments.[77] The DHHS was careful to note that the model contract was only to aid the parties in complying with the Privacy Rule, and the model contract's provisions were not necessary to comply under the Rule, nor was there any assurance that the model contract would comply with state law.[78] Further, the model contract does not contain provisions that may benefit the covered entity, but are not required to be in the contract under the Privacy Rule.[79] For these reasons, it is recommended that covered entities and business associates do not blindly utilize or incorporate the model contract terms into the their business associate contracts.

74. *Id.* § 164.504(e)(4)(ii)(A)-(B).
75. *Id.* § 164.504(e)(3).
76. *Id.*
77. Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. 14,776, 14,809 (Mar. 27, 2002).
78. *Id.*
79. *Id.*

IV. UNIQUE ISSUES CONFRONTING THE ATTORNEY-CLIENT RELATIONSHIP UNDER HIPAA

Within the sphere of issues that all business associates must face when addressing the Privacy Rule requirements[80] are those specific or unique requirements that exist between a business associate lawyer or law firm and a covered entity client. A number of these issues have no easy answer and will require fact-specific inquiry and analysis. This article, however, will attempt to address problems and conflicts that can arise in the attorney-client relationship.

A. THE ATTORNEY-CLIENT PRIVILEGE AND THE WORK PRODUCT DOCTRINE

One of the requirements under the Privacy Rule for business associate contracts is that business associates must make their internal practices, books, and records relating to the use or disclosure of PHI available for inspection by the DHHS.[81] This allows the DHHS to determine if covered entities are in compliance.[82]

In addition, business associates must allow individuals to access and amend their PHI if it was not compiled for a legal proceeding.[83] Note, however, that the Privacy Rule excludes the contractual requirements for business associates to provide access to the PHI or amendment of the PHI by individuals in situations involving PHI compiled in "reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding."[84] As such, an individual would not have direct access to PHI during legal proceedings, and it is less likely that the attorney-client privilege or the work product of the attorney would be violated in these limited situations. However, the attorney-client privilege and the work product doctrine may be jeopardized by the contractual provision granting the DHHS access to internal practices, books, and records.[85]

In general, the attorney-client privilege involves a situation where legal advice of any kind is sought from professional legal advisers in their capacity as such.[86] Clients' communications relating to that purpose are

---

80. Administrative Data Standards and Related Requirements, 45 C.F.R. § 164.504(e) (2002).

81. *Id.* § 164.504(e)(2).

82. *Id.*

83. *Id.* §§ 164.504(e)(2), 164.528(b).

84. *Id.* §§ 164.524(a), 164.526(a).

85. *Id.* § 164.504(e)(2)(ii)(H).

86. *See* United States v. Mass. Inst. of Tech. (MIT), 129 F.3d 681, 684 (1st Cir. 1997) (quoting 8 J. WIGMORE, EVIDENCE § 2292, at 554 (1961)).

made in confidence.[87] Finally, clients insist that the communications be permanently protected from disclosure by the legal advisers and are so protected unless the exception is waived.[88]

Whereas, the work product doctrine is designed to allow attorneys to "assemble information, sift what [they] consider[] to be the relevant from the irrelevant facts, prepare [their] legal theories and plan [their] strategy without undue and needless interference. . . . to promote justice and to protect their clients' interests."[89] Allowing the DHHS access to internal records could involve investigation into areas covered by the attorney-client privilege and the work product doctrine. If attorneys are required to produce the protected information, then the attorney-client privilege and the work product doctrine could be considered waived as to other parties.[90]

In *United States v. Massachusetts Institute of Technology (MIT)*,[91] the First Circuit addressed whether MIT's production of privileged documents to an auditing arm of the Department of Defense (DoD) resulted in a waiver of the attorney-client privilege and the work product doctrine as against the Internal Revenue Service (IRS) for the documents.[92] MIT had produced the documents to the DoD auditing agency as required by a contract between MIT and the agency to monitor compliance.[93] The IRS unsuccessfully sought the information from the auditing agency for an investigation into whether MIT was still a tax-exempt entity.[94] MIT argued that disclosing the information to the auditing agency was not "voluntary" and therefore, could not result in a waiver of the privilege, which would allow the IRS to obtain the documents.[95] The court disagreed with MIT's position:

> The extent of those pressures and constraints is far from clear, but assuming arguendo that they existed, MIT chose to place itself in this position by becoming a government contractor. In short, MIT's disclosure to the audit agency resulted from its own voluntary choice, even if that choice was made at the time it became a defense contractor and subjected itself to the alleged obligation of disclosure.[96]

---

87. *Id.*
88. *Id.*
89. Hickman v. Taylor, 329 U.S. 495, 511 (1947).
90. *See MIT*, 129 F.3d at 686-87.
91. 129 F.3d 681 (1st Cir. 1997).
92. *MIT*, 129 F.3d at 682.
93. *Id.* at 683.
94. *Id.*
95. *Id.* at 686.
96. *Id.* (footnote omitted) (citing *In re* John Doe Corp., 675 F.2d 482, 489 (2d Cir. 1982)).

Accordingly, the court concluded that MIT waived the attorney-client privilege, and the documents had to be produced.[97] The court then went on to hold that producing the documents to the auditing agency was a disclosure to an "adverse party," which destroyed any work product doctrine protection over the documents.[98]

The court determined that disclosing the documents to the auditing agency "was a disclosure to a potential adversary" even though the parties did not share a common legal interest and the disclosures were not part of a joint litigation.[99] "The audit agency was reviewing MIT's expense submissions. MIT doubtlessly hoped that there would be no actual controversy between it and the [DoD], but the potential for dispute and even litigation was certainly there. The cases treat this situation as one in which the work product protection is deemed forfeit."[100]

The Eighth Circuit has taken an opposite, and somewhat solitary, approach to waiving the attorney-client privilege. In *Diversified Industries, Inc. v. Meredith*,[101] the Eighth Circuit held that disclosing information to the government did not waive the protections of the attorney-client privilege or the work product doctrine with respect to a third party.[102] Subsequent courts have described this holding as creating a "selective" or "partial" waiver.[103] However, these courts, including a subsequent decision by the Eighth Circuit, have either called this holding into question or have expressly rejected it.[104]

A majority of cases have held that producing documents to a governmental agency may result in a waiver of the attorney-client privilege or the work product doctrine as against third parties.[105] Even where producing the information was involuntary because it was contractually required, the courts have held that the choice of entering into the contract was a

---

97. *Id.*

98. *Id.* at 687.

99. *Id.*

100. *Id.* (citing *In re* Steinhardt Partners, L.P., 9 F.3d 230, 234 (2d Cir. 1993), Westinghouse Elec. Corp. v. Republic of the Philippines, 951 F.2d 1414, 1428-31 (3d Cir. 1991), and *In re* Subpoenas Duces Tecum, 738 F.2d 1367. 1372 (D.C. Cir. 1984)).

101. 572 F.2d 596 (8th Cir. 1978).

102. *Meredith*, 572 F.2d at 611.

103. *E.g., In re* Columbia/HCA Healthcare Corp., 293 F.3d 289, 294-95 (6th Cir. 2002).

104. *Id.* at 303-04; *see also In re* Chrysler Motors Corp. Overnight Evaluation Program Litig., 860 F.2d 844, 847 (8th Cir. 1988) (holding that voluntarily producing documents to class action plaintiffs resulted in a waiver of the work product privilege as against the government, which was investigating the incident).

105. *See* United States v. Mass. Inst. of Tech. (MIT), 129 F.3d 681, 686 (1st Cir. 1997) (stating that most cases treat these situations as waiving the privileges).

voluntary action, and therefore, the provisions of the contract constituted a voluntary waiver of the privileges.[106]

With respect to the work product doctrine, courts have concluded that producing information was to an "adversary" because the disclosure of the protected information could have resulted in a dispute or litigation.[107] Once produced to an adversarial party, the work product protections are waived.[108]

Because a majority of cases have held that releasing protected information to a government party may result in a waiver as to all third parties,[109] it would be prudent for counsel to treat the production of internal practices, books, and records to the DHHS under the Privacy Rule as a waiver of the attorney-client privilege and the work product doctrine.[110] In order to attempt to counter this problem, an attorney must engage in careful drafting of the business associate contract. In addition, the possibility of legal action may be necessary to avoid divulging information that is otherwise protected under the attorney-client privilege or the work product doctrine.

One possible argument against divulging privileged information is that "internal practices, books, and records" does not include any information other than the PHI itself.[111] "Internal practices, books, and records"[112] are not defined under the Privacy Rule.[113] However, a lawyer could craft an argument that the DHHS only needs to review the immediate PHI and not all records of a business associate.

The counter to this argument is that the Privacy Rule requires disclosure of "internal practices, books, and records *relating to* the use and disclosure" of PHI.[114] The language of the Rule, on its face, does not limit the DHHS's access to only the actual PHI that was used or disclosed. The language appears to provide the DHHS access to all related books and records.[115] The phrase "internal practices"[116] also appears to require business associates to disclose the context in which the PHI was used or

106. *Id.*
107. *Id.* at 687.
108. *Id.*
109. *See id.* at 686-87.
110. Administrative Data Standards and Related Requirements, 45 C.F.R. § 164.504(e)(2)(ii)(H) (2002).
111. *Id.*
112. *Id.*
113. *Id.* § 160.103.
114. *Id.* § 164.504(e)(2)(ii)(H) (emphasis added).
115. *Id.*
116. *Id.*

disclosed. Further, even if an attorney successfully argued this interpretation, the PHI, in all forms, could still lose its privileged status.[117]

Another possible way to avoid waiving the attorney-client privilege or the work product doctrine is to argue that the Privacy Rule requirement is preempted by the privilege or the doctrine. To the extent that the attorney-client privilege and the work product doctrine are considered "state laws" they are only preempted as set forth under the Privacy Rule.[118] Under the preemption section of the regulations, "A standard, requirement, or implementation specification adopted under this subchapter that is contrary to a provision of State law preempts the provision of State law."[119] An exception to the preemption section allows a state law that is "more stringent" than the Privacy Rule to remain in full force.[120] However, the definition of "more stringent" set forth under the Privacy Rule seems to prevent a preemption argument based upon the attorney-client privilege or the work product doctrine.[121] The definition states:

> *More stringent* means, in the context of a comparison of a provision of State law and a standard, requirement, or implementation specification adopted under subpart E of part 164 of this subchapter, a State law that meets one or more of the following criteria:
>
> (1) With respect to a use or disclosure, the law prohibits or restricts a use or disclosure in circumstances under which such use or disclosure otherwise would be permitted under this subchapter, *except if the disclosure* is:
>
> (i) Required by the Secretary [of the DHHS] in connection with determining whether a covered entity is in compliance with this subchapter . . .[122]

Because the purpose of the business associate contractual requirement is to allow the DHHS to review business associates' records in order to determine whether covered entities are complying with the Privacy Rule,[123] the state law privilege or doctrine would likely be preempted by HIPAA.[124]

---

117. *See supra* notes 88-98 and accompanying text.
118. Administrative Data Standards and Related Requirements, 45 C.F.R. § 160.203 (2002).
119. *Id.*
120. *Id.* § 160.203(b).
121. *Id.* § 160.202.
122. *Id.* (emphasis added).
123. *Id.* § 164.504(e)(2)(ii)(H).
124. *Id.* § 160.203.

Another alternative may be to request an exception from the DHHS for the attorney-client privilege and the work product doctrine. Under the Privacy Rule, a request to except a provision of state law from preemption may be submitted to the DHHS through the state's "chief elected official," or a designee.[125] The request must be in writing, and it must set forth specific information about the excepted state law and why it should not be preempted.[126] Until the DHHS issues a determination on the issue of preemption, the Privacy Rule will apply.[127] To date, there has been no publicized request for an exception.

B. "MINIMUM NECESSARY" USE OR DISCLOSURE

Under the Privacy Rule, a use or disclosure to business associates must be limited to the "minimum necessary."[128] To carry out this requirement, covered entities must identify the people in their workforce who need access to PHI to carry out their duties.[129] Of those people identified who need access to PHI, covered entities must also list the category of PHI to which access is needed.[130] Covered entities must also develop policies and procedures designed to limit the disclosure of PHI,[131] and they must review requests for PHI on an individual basis.[132] Covered entities must limit any request for PHI to the minimum necessary.[133] For their own uses, disclosures, or requests, covered entities must only request what is necessary and not simply request the entire medical record, unless justified.[134]

Covered entities may rely upon their attorneys as to whether a request is for the minimum necessary if such reliance is reasonable under the circumstances and the information is requested for the purpose of providing professional services to the covered entity.[135] However, attorneys must represent that the information requested is the minimum necessary for the stated purpose.[136]

Thus, business associate attorneys may represent to covered entity clients that the request for information is only for the minimum necessary to

125. *Id.* § 160.204(a).
126. *Id.*
127. *Id.* § 160.204(b).
128. *Id.* § 164.502(b).
129. *Id.* § 164.514(d)(2)(i)(A).
130. *Id.* § 164.514(d)(2)(i)(B).
131. *Id.* § 164.514(d)(3)(i).
132. *Id.* § 164.514(d)(3)(ii)(B).
133. *Id.* § 164.514(d)(3)(ii)(A).
134. *Id.* § 164.514(d)(5).
135. *Id.* § 164.514(d)(3)(iii)(C).
136. *Id.*

carry out assignments. This could be accomplished by either a representation that a request is for the minimum necessary information each time an attorney requests PHI from a client,[137] or an attorney could incorporate the representation into the business associate contract and take steps internally to ensure that each individual request complies with the contractual representation.[138] If the business associate contract contains the blanket representation, the Privacy Rule would still appear to require covered entities to review the disclosures on an individual basis to determine whether a request is for the minimum necessary information.[139]

As a practical matter, it would seem a rare case where an individual's PHI would not be necessary for carrying out effective representation of a covered entity client. If the issue did not involve the individual's medical condition, then a case could be made out that disclosing the PHI would be unnecessary. However, in light of the liberal rules of discovery[140] and the Rules of Professional Responsibility,[141] most attorneys could make a legitimate argument for the provision of clients' PHI in a wide variety of cases. Accordingly, complete disclosure would likely be necessary for legal representation.

C. RETURN OR DESTRUCTION OF PHI

The business associate contract must provide that at the termination of the contract, if feasible, the business associate will return or destroy all PHI received from, or created or received by the business associate on behalf of the covered entity.[142] If the return or destruction of the PHI is not feasible, the business associate must extend the protections of the contract to the information and limit further uses or disclosures to those purposes that make the return or destruction infeasible.[143]

This requirement poses an interesting problem for lawyers that represent covered entity clients on several matters over long periods of time. Different jurisdictions may have different requirements for maintaining client files. In most cases, an attorney would be ill advised to immediately destroy case files upon completion of a specific project for a covered entity client. The same could be said for returning information to the client. For

137. *Id.*
138. *Id.* § 164.504(e)(2)(i).
139. *Id.* § 164.514(d)(3)(ii)(B).
140. FED. R. CIV. P. 26
141. MODEL RULES OF PROF'L CONDUCT R. 1.1 (1999).
142. Administrative Data Standards and Related Requirements, 45 C.F.R. § 164.504(e)(2)(ii)(I) (2002).
143. *Id.*

these reasons, an attorney would appear to have a strong argument that the immediate return or destruction would not be "feasible" under the Privacy Rule.[144] Attorneys must remember, however, that if the PHI is not returned or destroyed, then it must be protected under the Privacy Rule and further uses or disclosures must be limited, such as in a separate case or matter.[145]

D. CONFLICT OF INTEREST

The Privacy Rule requires many things of business associate attorneys. Some of these requirements arguably place attorneys in a conflict of interest with covered entity clients. For example, the contractual requirement that business associates provide the DHHS with access to their internal practices, books, and records relating to the use and disclosure of PHI appears to include information outside of that simply received from and provided to the individual covered entity client.[146] "Internal practices" could be construed to include attorneys' office practices, possibly even how attorneys have dealt with other covered and non-covered entities' health information.[147] These other clients may not want to turn over information to the DHHS and may wish to avoid the possibility that such production could result in a waiver of any attorney-client privilege or the work product doctrine.

Under the Model Rules of Professional Conduct, an attorney shall not reveal information relating to representation of a client unless the client consents after consultation.[148] Another client, covered entity or not, may not desire to disclose information to the DHHS. The other client may insist that the attorney fight to prevent such disclosure. In such a circumstance, by failing to produce the information to the DHHS, the business associate attorney is arguably breaching the business associate contract,[149] which could mean that the covered entity client, who is the target of the DHHS investigation, is in violation of the Privacy Rule.[150]

A conflict could even arise between the client and its attorney over information relating solely to that client and its PHI. Again, the contractual requirement goes beyond PHI and requires the business associate attorney

144. *Id.*
145. *Id.*
146. *Id.* § 164.504(e)(2)(ii)(H).
147. *Id.*
148. MODEL RULES OF PROF'L CONDUCT R. 1.6 (1999).
149. Administrative Data Standards and Related Requirements, 45 C.F.R. § 164.504(e)(2)(ii)(H) (2002).
150. *Id.* § 164.504(e)(1)(ii).

to produce information "relating" to the use or disclosure of PHI.[151] The internal practices, books, and records may be information that the attorney does not wish to produce to a governmental agency, especially in light of the potential waiver of any privilege claim as to that information.[152]

Under the Model Rules of Professional Conduct, a lawyer shall not represent a client if the representation of that client may be materially limited by the lawyer's responsibilities to another client, to a third party, or by the lawyer's own interests unless the lawyer and the client agree that the representation will not be adversely affected and consent is obtained.[153] Under the scenarios described above, another client, the DHHS, and the lawyer's own interests may materially limit the lawyer's representation of a client.

While it is not the author's opinion that the conflicting requirements of the Privacy Rule and the representation of clients necessarily require attorneys to withdraw or recuse themselves, it is the author's opinion that careful lawyers will utilize other counsel in drafting business associate contracts. Third-party attorneys or in-house counsel could be utilized in this manner to avoid the potential for a conflict in drafting the contract. Further, the use of in-house counsel or third-party attorneys will help ensure that clients are properly advised of their rights and that consent is obtained only after appropriate consultation.

V. CONCLUSION

The security and privacy regulations under HIPAA pose some difficult issues for attorneys who represent covered entity clients. The contractual requirements may place the attorney-client relationship in danger and allow attorneys' work product to be released. In addition, attorneys will need to maintain accurate records of all protected health information to comply with their contractual obligations. For these reasons, attorneys should carefully review the HIPAA Regulations and consult outside counsel where necessary.

---

151. *Id.* § 164.504(e)(2)(ii)(H).

152. *See* United States v. Mass. Inst. of Tech. (MIT), 129 F.3d 681, 686-87 (1st Cir. 1997) (determining that MIT's disclosure of information to the Department of Defense constituted a waiver of the attorney-client privilege and the work product doctrine in regards to the IRS).

153. MODEL RULES OF PROF'L CONDUCT R. 1.7 (1999).

***