HIPAA IN REAL TIME: PRACTICAL IMPLICATIONS OF THE FEDERAL PRIVACY RULE

Diane Kutzko, Gilda L. Boyer,** Deborah J. Thoman*** & Nicholas L. Scott*****

TABLE OF CONTENTS

---

* Diane Kutzko is a senior member of Shuttleworth & Ingersoll, P.L.C., in Cedar Rapids, Iowa. Ms. Kutzko received her B.A. in 1967 from Brooklyn College and her J.D. in 1981 from the University of Iowa College of Law.

** Gilda L. Boyer is a senior member of Shuttleworth & Ingersoll, P.L.C., in Cedar Rapids, Iowa. Ms. Boyer received her B.S.S. in 1984 from Cornell College and her J.D. in 1991 from the University of Iowa College of Law.

*** Deborah J. Thoman is the Compliance/Privacy Officer at the University of Iowa Hospitals and Clinics in Iowa City, Iowa. Ms. Thoman received her B.A. from the University of Iowa in 1977 and her M.A. from the University of Iowa in 1994.

**** Nicholas L. Scott is an associate at Shuttleworth & Ingersoll, P.L.C., in Cedar Rapids, Iowa. Mr. Scott received his B.A. from the University of Northern Iowa in 1998 and his J.D. in 2001 from the University of Iowa College of Law.

I. INTRODUCTION

The Health Insurance Portability and Accountability Act of 1996 [hereinafter the Act or HIPAA][1] contains the first comprehensive federal privacy rule protecting an individual's medical information. This Federal Privacy Rule [hereinafter Privacy Rule] covers medical information maintained either on paper or electronically.[2] It also applies to oral communications concerning medical information.[3] After April 14, 2003, the implementation date of the Privacy Rule, the use and disclosure of confidential medical information in the hands of health care providers and payers (federal payers, including Medicare, Medicaid, and private health insurers), and those other individuals and entities defined as "covered entities," will be governed by the Privacy Rule.[4] Much existing state law, and therefore provider and payer practices, will be preempted by the Privacy Rule.[5] Because the Privacy Rule acts as a confidentiality "floor," however, state laws that are more protective of a patient's medical information will not be preempted by the Privacy Rule.[6] In addition, the drafters of the Act made a policy decision to effectively exempt out state workers' compensation statutes, such as Iowa Code Chapter 85.[7] Therefore, health insurers and health care providers will have to navigate their way through the requirements of both the Privacy Rule and their respective state laws. Further complicating matters, the

---

1. Health Insurance Portability and Accessibility Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996) [hereinafter HIPAA of 1996]; *see also* 45 C.F.R. §§ 160, 164 (2002). The Office for Civil Rights (OCR), a branch of the Department of Health and Human Services, has been charged with enforcement of the Privacy Rule, and has issued several publications which are referred to as "Guidances." These publications elaborate on the intent of the Privacy Rule. OFFICE FOR CIVIL RIGHTS, STANDARDS FOR PRIVACY OF INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION (July 21, 2002) [hereinafter July 21, 2002 Guidance]; OFFICE FOR CIVIL RIGHTS, STANDARDS FOR PRIVACY OF INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION, *at* http://www.hhs.gov/ocr/hipaa/guidelines/guidanceallsections.pdf (Dec. 3, 2002) [hereinafter Dec. 3, 2002 Guidance]. The July 21, 2002 Guidance has been removed from the OCR's website, perhaps because it was viewed as superseded by the issuance of the "final, final" Rule in August 2002.

2. 45 C.F.R. pts. 160 and 164.

3. *See id.* §§ 160.103, 164.501.

4. *Id.* §§ 160.102-160.103.

5. *See* discussion *infra* Part III.C (analyzing the Act's preemption principles).

6. Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. 53,182 (Aug. 14, 2002) (to be codified at 45 C.F.R. pts. 160, 164); 45 C.F.R. § 160.201.

7. *See* 45 C.F.R. § 164.512(l) (stating that "[a] covered entity may disclose protected health information as authorized by and to the extent necessary to comply with laws relating to workers' compensation or other similar programs, established by law, that provide benefits for work-related injuries or illness without regard to fault"); *see also* IOWA CODE ch. 85 (2003).

Privacy Rule has gone through a number of significant changes from the time it was issued as a proposed rule in 1999.[8]

The Privacy Rule is deceptively simple to state: "A covered entity may not use or disclose [an individual's] protected health information, except as permitted or required by [the Privacy Rule]."[9] However, the cliché, "the devil is in the details," has never been more applicable.

Part II of this Article gives a general overview of the Privacy Rule's origin. Part III discusses the areas covered by the Privacy Rule and what state laws have been left in place. Part IV addresses the practical problems that will be involved in the Privacy Rule's implementation, specifically focusing on the impact it will have on employer group health plans and the insurance industry.[10] This Article is intended to provide guidance to those whose business practices will be affected by the Privacy Rule, to highlight some of the areas that will need to be monitored, and to examine the issues that will ultimately need to be resolved. Finally, Part V focuses on patients—one class of individuals for whom the Privacy Rule was arguably originally intended—taking the reader through a course of treatment to illustrate how the new Privacy Rule will and will not change the uses and disclosures of patient information.

II. THE GENESIS AND EVOLUTION OF THE FEDERAL PRIVACY RULE

A. *The Health Insurance Portability and Accountability Act of 1996*

In 1996, the United States Congress passed the Health Insurance Portability and Accountability Act.[11] The Act was, in part, a response to the Clinton Administration's efforts to "fix" the health care system which, rightly or wrongly, many Americans perceived as being broken.[12] The primary thrust of the Act was to increase access to health care through expanded portability and renewability of insurance.[13]

---

8. *See generally* Standards for Privacy of Individually Identifiable Health Information, 64 Fed. Reg. 59,918 (Nov. 3, 1999) (codified at 45 C.F.R. §§ 160.101-164.534).

9. 45 C.F.R. § 164.502(a).

10. *See* discussion *infra* Part IV (examining how the Act affects those plans and illustrating how problematic compliance will be for the insurance industry).

11. HIPAA of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996).

12. *See generally* James Cordone, *Health Care Reform in the 1990's from the Clinton Plan to Kassebaum-Kennedy*, 3 CONN. INS. L.J. 193 (1996).

13. *See id.* at 206-10 (stating that the primary goal of the Act—on the issue of portability—was to allow for Americans who might lose their health insurance to enroll in individual plans, and that the goal of renewability was to guarantee automatic renewal of individual and group health care plans).

Tucked into the Act were "administrative simplification" provisions.[14] This term seems ironic at best, given the perceived and actual burden those provisions would ultimately impose on the industry, providers, and payers alike. The intent of these provisions was to improve the efficiency and effectiveness of the nation's health care system, including payment as well as treatment through the development of a health information system.[15] The cornerstone of that system was the electronic record, which was believed in the 1990s to be the future key to the efficient delivery of health care.[16]

The Act required the establishment of unique health identifiers for employers, health plans, health care providers, and individuals.[17] The Act further required the establishment of standard code sets and transactions for the electronic transmission of health information, as well as the promulgation of security standards and privacy standards for individually identifiable health information.[18]

The Act required the Secretary of Health and Human Services [hereinafter Secretary] to submit recommendations to Congress regarding standards for the privacy of individually identifiable information.[19] The Act further imposed on Congress a deadline of thirty-six months from the effective date of the Act to pass privacy legislation.[20] In the event that Congress failed to pass such legislation within thirty-six months of the Act's enactment date, the Secretary was directed to promulgate final privacy regulations within forty-two months of the Act's effective date.[21]

Due to the fact that Congress missed its self-imposed deadline for the enactment of medical privacy legislation, responsibility fell to then-Secretary Donna Shalala to promulgate the required privacy standards through her

---

14. HIPAA of 1996, Pub. L. No. 104-191, §§ 261-264, 110 Stat. 2021-34 (1996).

15. Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. 53,182 (Aug. 14, 2002) (to be codified at 45 C.F.R. pts. 160, 164). As the Preamble to the Final Privacy Rule states:

> HIPAA's Administrative Simplification provisions . . . were designed to improve the efficiency and effectiveness of the health care system by facilitating the electronic exchange of information with respect to certain financial and administrative transactions carried out by health plans, health care clearinghouses, and health care providers who transmit information electronically in connection with such transactions.

Id.

16. *See id.*

17. HIPAA of 1996, Pub. L. No. 104-191, § 262, 110 Stat. 2024-26.

18. *Id.*

19. *Id.* § 264(c)(1).

20. *Id.*

21. *Id.*

rulemaking authority.[22] The proposed rule was issued in November 1999.[23] It generated an estimated fifty-two thousand comment letters.[24] The "final rule" was issued on December 28, 2000.[25] On March 27, 2002, a notice of proposed rule making (NPRM), perhaps reflecting a shift in administrations, was issued by the current Secretary, Tommy Thompson.[26] Again, a number of changes were proposed, increasing the uncertainty of what the "final, final" rule would look like. That rule was issued in August 2002,[27] with significant modifications, leaving approximately eight months for insurers, providers, and other individual entities covered by the Privacy Rule to comply.

B. *The Rationale for the Federal Privacy Rule—Perceived or Actual Patient Concerns About Privacy of Medical Information in an Increasingly Complex Health Delivery System*

A patient's right to privacy has long been protected by state law[28] and certain federal laws and regulations.[29] In addition, many health professionals have long been covered by ethical principles of confidentiality.[30] The issue of the adequacy of such protections began to receive increased public attention in the 1990s.

---

22. Anthony C. Colletti & Tracey Sorens Pachman, *HIPAA: An Overview*, 13 No. 1 HEALTH LAW. 14 (2000).

23. Standards for Privacy of Individually Identifiable Health Information, 64 Fed. Reg. 59,918-60,065 (Nov. 3, 1999) (codified at 45 C.F.R. pts. 160, 164).

24. Some believed that forty-five thousand of these were form letters. *Proposed Rule on the Privacy of Individually Identifiable Health Information: Hearing Before the Senate Comm. on Health, Education, Labor, and Pensions*, 106th Cong. 2 (2000) (opening statement of Senator Jeffords, Chairman, Senate Committee on Health, Education, Labor, and Pensions).

25. Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462-82,565 (Dec. 28, 2000) (codified at 45 C.F.R. §§ 160.101-164.534).

26. Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. 14,776 (Mar. 27, 2002) (to be codified at 45 C.F.R. pts. 160, 164).

27. Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. 53,182 (Aug. 14, 2002) (to be codified at 45 C.F.R. pts. 160, 164).

28. *See, e.g.*, IOWA CODE § 622.10 (2003) (providing for physician-patient privilege); McMaster v. Iowa Bd. of Psychology Exam'rs, 509 N.W.2d 754, 758 (Iowa 1993) (holding that the right to privacy in medical records is constitutionally protected).

29. *E.g.*, Federal Privacy Act of 1974, 5 U.S.C. § 552a (2000); Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g (2000); 42 C.F.R. pt. 2 (2002).

30. *See, e.g.*, COUNCIL ON ETHICAL AND JUDICIAL AFFAIRS, AM. MED. ASS'N, CODE OF MEDICAL ETHICS: CURRENT OPINIONS WITH ANNOTATIONS §§ 5.05, 5.055, 5.057, 5.06, 5.07, 5.075, 5.08, 5.09 (2002) (discussing confidentiality, confidential care for minors, confidentiality of HIV status on autopsy reports, confidentiality of attorney-physician relationship, confidentiality with regard to computers, confidentiality of records disclosed to collection companies, confidentiality with regard to insurance company representatives, and confidentiality with regard to industry-employed physicians and independent medical examiners, respectively).

The heightened public concern was due in part to the growing importance of the electronic medical record in an increasingly complicated health delivery system.[31] For example, a study by the National Research Council, conducted at the time hearings were being conducted by the Senate on the privacy regulations, found that "the pathway of a typical medical record is no longer confined within the control of the patient's personal physician. Today, a typical record may be handled by numerous individuals in more than 17 different organizations."[32] A Health Information Privacy Survey prepared by Louis Harris and Associates in 1993 found that fifty-six percent of the public favored the enactment of comprehensive federal legislation governing the privacy of health care information, and eighty-five percent of the public said that protecting the confidentiality of medical records was absolutely essential or very important to them.[33] In addition, ninety-six percent of the public wanted penalties imposed for unauthorized disclosure of medical records, and also desired guaranteed access to their own health records.[34]

The increased public concern was fueled by a number of well-publicized egregious breaches of confidentiality. For example, in the mid-1990s a New York Congresswoman won her House seat in spite of the fact that her medical records, which included descriptions of a bout with depression and an attempted suicide, were faxed to New York media during the campaign.[35] In another well-publicized incident, federal auditors demanded the names of patients seeking confidential AIDS treatment at a Boston clinic, and then disclosed the information to other federal agencies.[36] Further, HMOs were discovered to have engaged in the practice of sending letters to employers detailing the health problems of their employees.[37]

The issue remains open as to whether the Privacy Rule, as implemented, will in fact accomplish its goal of protecting patient confidentiality by preventing

---

31. *See* Lawrence O. Gostin & James G. Hodge, Jr., *Personal Privacy and Common Goods: A Framework for Balancing Under the National Health Information Privacy Rule*, 86 MINN. L. REV. 1439, 1440 (2002) (noting "the ongoing shift from paper to electronic records within the national health information infrastructure").

32. *Proposed Rule on the Privacy of Individually Identifiable Health Information: Hearing Before the Senate Comm. on Health, Education, Labor, and Pensions*, 106th Cong. 2 (2002) (opening statement of Senator Jeffords, Chairman, Senate Committee on Health, Education, Labor, and Pensions).

33. Prepared Statement of Janlori Goldman, Deputy Director, Center for Democracy and Technology submitted to the Subcomm. on Gov't Mgmt. Info. and Tech. of the House Comm. on Gov't Reform and Oversight, *at* 1996 WL 329690 (citations omitted).

34. *Id.*

35. *Id.*

36. *Id.*

37. *Id.*

or eliminating the abuses (or perceived abuses) that gave rise to its enactment.[38] For example, as discussed below, the general practice of requiring consent for disclosure has been supplanted with a "notice of privacy practices," which, if drafted to be compliant with the Privacy Rule, may be lengthy. Once the patient is presented with the notice on a one-time basis prior to a patient's first episode of care or enrollment in a health plan, the provider or health plan may disclose protected health information for treatment, payment, and the health care operations of the provider or health plan without further notice or opportunity to object.[39] It may also disclose information for law enforcement and public health purposes.[40] It is not clear that the one-time notice, provided at admission when a patient's stress level is high and when he or she does not necessarily have the time to comprehend the scope of disclosure, is sufficient to form the basis of a knowing relinquishment of the confidentiality of the information.[41] As discussed in Part V, from a patient's perspective, and in practice, the Privacy Rule may simply not accomplish what it set out to do.

III. AN OVERVIEW OF THE FEDERAL PRIVACY RULE

A. *HIPAA Basics—Defined Terms*

As discussed above, the Privacy Rule governs the use and disclosure of "protected health information" in the hands of "covered entities," which are "health care providers," "health plans," and "health care clearinghouses."[42] These terms, as well as a number of others are defined in the Privacy Rule in a precise manner, and are often given a meaning somewhat different than their common meaning. Indeed, the Privacy Rule is difficult in its application in large part because of the number of new, defined terms that it introduces.[43] The

---

38. *See generally* Peter D. Jacobson, *Medical Records and HIPAA: Is It Too Late to Protect Privacy?*, 86 MINN. L. REV. 1497 (2002).

39. 45 C.F.R. § 164.520 (2002) (providing the standard and implementation standards for the notice of privacy practices required by the Privacy Rule); *see also* discussion *infra* Part III.B. To the extent that state law is more protective of patients' rights, authorization or consent may still be necessary. *See* discussion *infra* Part III.B.2.

40. *See* discussion *infra* Part III.B.

41. A recent analysis has evaluated a number of privacy notices as to their "readability." One of the requirements of a notice is that it be in plain language. 45 C.F.R. § 164.520(b)(1). The analysis found that the average reading level of the notices was second to third-year college. *See* Mark Hochhauser, *Readability of HIPAA Privacy Notices*, *at* http://www.benefitslink.com/articles/hipaareadability.pdf (Mar. 12, 2003).

42. 45 C.F.R. § 160.102(a)(1).

43. *See* Jacobson, *supra* note 38, at 1504 ("[T]he HIPAA regulations are so complex that they may simply collapse of their own weight. They are very difficult to follow, so that even well-intended health care administrators may be unable to decipher their meaning.").

following is a brief summary of the defined terms that are the building blocks of the Privacy Rule.

1. *Protected Health Information*

Traditionally, providers, insurers, and others in the health care industry have thought of confidentiality protections extending to the "medical record" or "medical chart."[44] The Act defines and extends the scope of what is protected health information (often termed "PHI"). Notably, it extends the definition, and perhaps enlarges the confidentiality protection to payment and billing information. "Protected health information" is any individually identifiable information concerning the past, present, or future physical or mental health or condition of an individual;[45] the provision of health care to an individual; or the past, present, or future payment for that provision of health care to an individual.[46] Further, the Privacy Rule covers protected health information in any form—whether it is oral, written, or electronically created and transmitted.[47]

2. *Covered Entities*

Because the Privacy Rule provides that protected health information in the hands of a covered entity must be used or disclosed as provided by the Privacy Rule,[48] it is essential to determine whether an entity is a covered entity in the first instance.[49] Merely because protected health information is involved does not

---

44. A number of states have statutes defining the scope of a medical record. *See, e.g.*, WIS. STAT. § 146.81(4) (1997) (defining patient health care records). Iowa does not have such a statute, and the scope of what constitutes the medical record has been more an issue of professional practice and general understanding within the health care industry.

45. Protected health information is by its nature "individually identifiable." 45 C.F.R. § 164.501. The Privacy Rule does provide for circumstances under which such information can be "de-identified" and therefore used or disclosed less restrictively. *Id.* § 164.514; *see also* discussion *infra* Part III.B.4.

46. 45 C.F.R. § 164.501.

47. *Id.*

48. *Id.* § 164.500.

49. In recognition of the increasing complexity of the way health care is delivered and paid for, the Secretary, in drafting the Privacy Rule, provides specific standards for a variety of delivery systems. *See id.* § 164.504 ("Uses and disclosures: Organizational requirements"); *id.* § 164.501 (defining an "organized health care arrangement"). The three major categories of organizational configurations are "hybrid entities," "affiliated covered entities," and "organization health care arrangements." *See id.* §§ 164.501, 164.504(a), (d). With regard to "hybrid entities," the Secretary has stated:

> In the final rule we address the issue of differentiating health plan, covered health care provider and health care clearinghouse activities from other functions carried out by a single legal entity in paragraphs (a-c) of § 164.504. We have created a new

make a use or disclosure fall under the protections of the Act. It must be in the hands of a covered entity.[50]

The scope of coverage of the Privacy Rule derives from those entities that were covered by the Act.[51] Covered entities include those health care providers who conduct certain financial and administrative transactions electronically, including billing to governmental entities.[52] "Providers" include all entities that provide health related services as well as products, and specifically include pharmacists and durable medical equipment providers.[53] Under the Act, only those providers who transmit "any health information in electronic form," that is, those who bill electronically whether it be to Medicare or Medicaid, are covered by the Privacy Rule.[54] However, for any provider who does so, all protected health information, including oral or paper communications or records, will be covered.[55]

> term, "hybrid entity," to describe the situation where a health plan, health care provider, or health care clearinghouse is part of a larger legal entity; under the definition, a "hybrid entity" is "a single legal entity that is a covered entity and whose covered functions are not its primary functions."

Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462, 82,502 (Dec. 28, 2000) (codified at 45 C.F.R. § 164.504(a)).

"Affiliated covered entities" are legally separate covered entities under common ownership or control. 45 C.F.R. § 164.504. An "organized health care arrangement" includes a "clinically integrated care setting in which individuals typically receive health care from more than one health care provider" and an "organized system of health care in which more than one covered entity participates." *Id.* § 164.501. While there are certain advantages as explained in the Privacy Rule, a potential danger exists in separate corporate entities holding themselves out as one entity. Notably, participants in such entities for purposes of the Act may be subject in future unrelated litigation to joint and several liability.

50. Employers, as an example, are generally not covered entities, except to the extent that employer health plans bring them under the umbrella of "health plans." *See* discussion *infra* Part IV.

51. 45 C.F.R. § 160.102.

52. *Id.*

53. *Id.*

54. *Id.*

55. A number of comments to the original final Privacy Rule, published in December 2000, questioned the Secretary's authority to regulate medical information in nonelectronic form. Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462, 82,619 (Dec. 28, 2000). However, the Act does define "protected health information" to include all forms of such information, perhaps weakening the argument that the Secretary has exceeded his scope in this area. HIPAA of 1996, Pub. L. No. 104-191, § 262, 110 Stat. 2022 (1996) (codified at 42 U.S.C. § 1320(d) (2000)). More troublesome is the issue of the Secretary's authority over noncovered entities who render services to or on behalf of providers, so-called "business associates," discussed *infra* at Part III.A.5. It is clear that the "business associate" relationship extends the requirements of the Act to individuals and entities never contemplated by Congress to be covered entities under the Act.

The term "covered entity" also includes "health plans," which are defined as: "individual or group plans that provide, or pay the cost of, medical care."[56] Health plans include, but are not limited to: (1) group health plans (excluding plans that are administered by the employer, and plans with under fifty members); (2) health insurers; (3) parts A and B of the Medicare program; (4) the Medicaid program; (5) issuers of a long term care policy, including a nursing home fixed-indemnity policy; and (6) any employee welfare benefit plan.[57] While private health care insurers are included, life insurers, disability insurers, and workers' compensation insurers are not.[58]

The third class of covered entities are health care clearinghouses, which are defined as any entity that "(1) [p]rocesses or facilitates the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction"; or "(2) receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity," for example, billing services.[59]

3. *Treatment, Payment, and Health Care Operations*

Treatment, payment, and health care operations, sometimes shortened to "TPO," are precisely defined under the Privacy Rule. "Treatment" is defined by the Privacy Rule in relevant part as "the provision, coordination, or management of health care and related services by one or more health care providers"; "consultation between health care providers relating to a patient"; or the "referral of a patient for health care from one provider to another."[60] "Payment" is defined as activities undertaken by a health plan to determine its responsibilities for coverage under the health plan, or by a health care provider to obtain or provide reimbursement for the provision of health care.[61] "Health care operations" are administrative and operational functions performed by the covered entity's work force.[62] Health care operations include, but are not limited to: (1) quality assessment and improvement; (2) review of the competency or qualifications of health care professionals; (3) underwriting and experience rating in connection with the renewal of an existing contract of insurance with respect to individuals

---

56. 45 C.F.R. § 160.503.
57. *Id.* § 160.103.
58. *See id.*
59. *Id.*; *see also* discussion *infra* Part IV (discussing clearinghouses in the context of employer health plans).
60. 45 C.F.R. § 164.501.
61. *Id.*
62. *Id.*

who are already enrolled in the health plan; (4) medical review and auditing; (5) compiling or analyzing information in anticipation of or for use in a civil or criminal legal proceeding; (6) business planning and development; and (7) management activities.[63]

4. *Minimum Necessary Information*

The Privacy Rule introduces the principle of "minimum necessary" information both for internal uses of protected health information and external disclosures. The Privacy Rule provides as follows:

> When using or disclosing protected health information or when requesting protected health information or when requesting protected health information from another covered entity, a covered entity must make reasonable effort to limit protected health information to the minimum necessary to accompany the intended purpose of the use, disclosure, or request.[64]

Under the final Rule as revised, the "minimum necessary" standard does not apply to certain disclosures. The exceptions include: (1) disclosures to or requests by a health care provider for treatment purposes; (2) disclosures to the individual who is the subject of the information; and (3) uses or disclosures made pursuant to an individual's authorization.[65] For disclosures covered by the standard, a covered entity is required to take "reasonable steps" to ensure that only the "minimum necessary" information to accomplish the intended purposes is disclosed.[66] The final Rule is an improvement over the proposed Privacy Rule in that the latter required an independent evaluation of each request for disclosure, including those made for treatment and authorization.[67]

For internal uses of protected health information, "the covered entity's policies and procedures must identify the persons or classes of persons within the covered entity who need access to the information to carry out their job duties, the categories or types of protected health information needed, and conditions appropriate to such access."[68] When it comes to internal uses of information,

---

63. *Id.*
64. *Id.* § 164.502(b).
65. *Id.* § 164.502(b)(2); Dec. 3, 2002 Guidance, *supra* note 1, at 22.
66. 45 C.F.R. § 164.502(b)(1).
67. *See* Standards for Privacy of Individually Identifiable Health Information, 64 Fed. Reg. 59,918, 60,054 (Nov. 3, 1999) (not including situations where the minimum necessary standard does not apply, which the final Privacy Rules did include).
68. Dec. 3, 2002 Guidance, *supra* note 1, at 22.

"minimum necessary" is equated with information for which there is a need to know.[69]

For routine requests and disclosures, "the policies and procedures may be standard protocols and must limit the protected health information disclosed or requested to that which is the minimum necessary for that particular type of disclosure or request."[70] For nonroutine disclosures, covered entities must develop a protocol for determining what is "minimally necessary" on a case-by-case basis.[71] The standard applies to disclosures to entities that provide services to and on behalf of covered entities, that is, business associates,[72] and is particularly problematic in the context of employer health plans.

The standard has been softened somewhat in the Guidance issued by the OCR, which states that a covered entity may rely on the representation of another covered entity for what is minimally necessary, thus eliminating the need for an independent inquiry.[73] For example, an independent inquiry by a health care provider is unnecessary when an insurer requests information for claims processing purposes. Further, perhaps in recognition of the continuing difficulty of making these determinations, the OCR has stated in its Guidance that the Department of Health and Human Services will continue to provide clarification of this standard, and to "monitor the workability of the minimum necessary standard and consider proposing revisions, where appropriate, to ensure that the Privacy Rule does not hinder timely access to quality health care."[74]

5. *Business Associates*

The Privacy Rule recognizes the realities of the health care environment to the extent that covered entities "do not carry out all of their health care activities and functions by themselves," but instead use individuals and entities that provide services to them or on their behalf, using the protected health information of the covered entity.[75] These individuals or entities are "business associates."[76] In general terms, these are entities and individuals who are not part

---

69. *See id.* at 19 (explaining, as an example, that the "covered entities policies and procedures must identify the persons or classes of persons within the covered entity who need access to the information to carry out their job duties").
70. *Id.*
71. 45 C.F.R. §§ 164.502(b), 164.514(d); Dec. 3, 2002 Guidance, *supra* note 1, at 22.
72. 45 C.F.R. § 164.514(d); Dec. 3, 2002 Guidance, *supra* note 1, at 24.
73. Dec. 3, 2002 Guidance, *supra* note 1, at 22.
74. *Id.*
75. *Id.* at 34.
76. 45 C.F.R. §§ 164.502(e)(1), 164.504(e)(1), 164.532(d)-(e).

of the covered entities' work force,[77] but perform certain functions. Exactly who such entities or individuals are has created considerable confusion. The Privacy Rule gives examples of business associate functions and activities. These examples include "claims processing or administration, data analysis, processing or administration, . . . quality assurance, billing, benefit management, . . . [and] practice management."[78] The Privacy Rule also gives examples of functions and activities, which include legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, and financial services to the extent that these services involve the use or disclosure of protected health information.[79] The Privacy Rule excepts out certain disclosures, including disclosures by a covered entity to a health care provider for treatment of the individual, disclosures to a health plan sponsor, such as an employer by a group health plan,[80] and the collection and sharing of protected health information by governmental entities such as Medicare and Medicaid.[81]

The Privacy Rule ensures that covered entities will not escape coverage under the Act by contracting away their HIPAA-covered functions, such as treatment, payment, or health care operations. It requires a covered entity to receive "satisfactory assurance[s]" from its business associates that the business associate will "appropriately safeguard the protected health information it receives or creates on behalf of the covered entity."[82] Those "satisfactory assurance[s]" must be in writing, in the form of a "business associate agreement."[83] The agreement essentially requires the business associate to comply with the requirements of the Act.[84]

The final Rule, as revised, lessens the burden on covered entities for the conduct of what the proposed Rule termed "business partners."[85] The Privacy Rule, as proposed, imposed on covered entities the responsibility of monitoring

---

77. "Work force" is defined as "employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity." *Id.* § 160.103.

78. *Id.*

79. *Id.*

80. *Id.* For further discussion of this example, see *infra* Part III.

81. 45 C.F.R. § 164.502(e)(1)(ii)(c); Dec. 3, 2002 Guidance, *supra* note 1, at 42.

82. 45 C.F.R. § 164.502(e)(1)-(2); Dec. 3, 2002 Guidance, *supra* note 1, at 39.

83. 45 C.F.R. § 164.502(e); Dec. 3, 2002 Guidance, *supra* note 1, at 39.

84. The OCR provides sample business associate contract language on its website. *See* OCR, SAMPLE BUS. ASSOC. CONTACT PROVISIONS, *available at* http://www.hhs.gov/ocr/hipaa/contractprov.html (Aug. 14, 2002); *see also* Dec. 3, 2002 Guidance, *supra* note 1, at 40-41 (providing examples of what a business associate contact must contain).

85. See the discussion of the history of the business associate standard in Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462, 82,475-82,476 (Dec. 28, 2000) (codified at 45 C.F.R. § 160.103).

the activities of so-called business partners. Specifically, covered entities were liable for the breaches of their business partners if they "knew or should have known" of improper use of protected health information and failed to take reasonable steps to cure a breach of the business partner contract or terminate the contract.[86] The final Rule softens this burden by penalizing covered entities for the acts of their now-termed business associates only if the covered entity has actual knowledge of the breach.[87]

The issue of extending the requirements of the Act to noncovered entities raises serious questions as to whether the Secretary has exceeded his authority and jurisdiction. Certainly, the concept of "business associates" extends the protections of the Privacy Rule well beyond the covered entities as defined in the Act, from which the Secretary's rulemaking authority derives.[88]

The drafters of the Privacy Rule vigorously and summarily rejected the arguments that requiring "satisfactory assurance" of compliance with the Act was tantamount to subjecting noncovered entities to the jurisdiction of the Privacy Rule. As stated in the Preamble to the Privacy Rule:

> With regard to our authority to require business associate contracts, we clarify that Congress gave the Department explicit authority to regulate what uses and disclosures of protected health information by covered entities are "authorized." If covered entities were able to circumvent the requirements of these rules by the simple expedient of contracting out the performance of various functions, these rules would afford no protection to individually identifiable health information and be rendered meaningless. It is thus reasonable to place restrictions on disclosures to business associates that are designed to ensure that the personal medical information disclosed to them continues to be protected and used and further disclosed only for appropriate (i.e., permitted or required) purposes.[89]

The OCR similarly (and conclusorily) rejected the assertions that the Secretary exceeded his authority:

---

86. Standards for Privacy of Individually Identifiable Health Information, 64 Fed. Reg. 59,918, 60,055 (Nov. 3, 1999).

87. Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462, 82,476 (Dec. 28, 2000) (providing that if the "covered entity finds out about a material breach" it must take "reasonable steps to cure the breach or end the violation"); *see also* Dec. 3, 2002 Guidance, *supra* note 1, at 46.

88. HIPAA of 1996, Pub. L. No. 104-191, § 262, 110 Stat. 2021-23 (1996) (codified at 42 U.S.C. § 1320(d) (2000)). The Act defined covered entities as health care providers, health plans, and health care clearinghouses. *See id.*

89. Standard for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. at 82,640-641.

> The Health Insurance Portability and Accountability Act of 1996 (HIPAA) gives the Secretary authority to directly regulate health plans, health care clearinghouses, and certain health care providers. It also grants the Department explicit authority to regulate the uses and disclosures of protected health information maintained and transmitted by covered entities. Therefore, the Department does have the authority to condition the disclosure of protected health information by a covered entity to a business associate on the covered entity's having a written contract with that business associate.[90]

The OCR also rejected the argument that the Act does not "pass through" its requirements to business associates:

> The HIPAA Privacy Rule does not "pass through" its requirements to business associates or otherwise cause business associates to comply with the terms of the Rule. The assurances that covered entities must obtain prior to disclosing protected health information to business associates create a sort of contractual obligations far narrower than the provisions of the Rule, to protect information generally and helps the covered entity comply with its obligations under the Rule.[91]

This is disingenuous. The Privacy Rule clearly "passes through" duties imposed on the covered entity to business associates by requiring written contracts with noncovered entities.[92] For example, the Privacy Rule contractually imposes on business associates the duties imposed by the Privacy Rule on covered entities, such as the duty to comply with the patient's right of access to his or her information, right to seek an amendment, and the right to an accounting of protected health information in the hands of a covered entity.[93]

6. *Designated Record Set*

A designated record set is:

> (1) A group of medical records maintained by or for a covered entity that is:
> (i) The medical records and billing records about individuals maintained by or for a covered health care provider;
> (ii) The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or

---

90. Dec. 3, 2002 Guidance, *supra* note 1, at 44.
91. *Id.*
92. *See* 45 C.F.R. § 164.502(e)(2) (2002).
93. *Id.* § 164.504(e).

(iii) Used, in whole or in part, by or for the covered entity to make decisions about individuals.[94]

The "designated record set" is not equivalent to the entire medical record.[95] For example, it may contain radiology reports, but not actual diagnostic films.[96]

The concept of a designated record set is important to the Privacy Rule in that it serves to limit the rights of patients. Patients have a right to access and amendment, but that right does not extend to all of their protected health information, it only extends to what the covered entity deems to be within the "designated record set."[97] Further, the Privacy Rule exempts from the designated record set certain records, the most important of which is psychotherapy notes.[98] This results in a limitation on patient rights that initially looks far broader than it actually is.[99]

B. *HIPAA Basics—Disclosing Protected Health Information Under the Act*

After April 14, 2003, the implementation date for the Privacy Rule, the manner in which providers, health plans, and other covered entities and their "business associates" will use and disclose protected health information will change. Whether the changes are for the better, that is, either more protective of a patient's privacy rights, or more efficient from a covered entity's standpoint, remains to be seen. The following is not an exhaustive discussion of those uses and disclosures,[100] rather it is a discussion focusing on the shift away from consent in the treatment and payment setting, as well as an examination of some of the other changes that providers and health plans may most frequently encounter, including disclosures by authorization and disclosures in the litigation context.

---

94. *Id.* § 164.501.

95. Gwen Hughes, *Defining the Designated Record Set (AHIMA Practice Brief), available at* http://www.library.ahima.org/xpedio/groups/public/documents/ahima/pub_bok1_017122.html (last visited Mar. 4, 2003).

96. *See id.*

97. 45 C.F.R. §§ 164.524, 164.526.

98. "Psychotherapy notes" are defined as "notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual's medical record." *Id.* § 164.501. Additionally, patients do not have the right to access or amend either protected health information compiled during the course of litigation, or clinical lab results under the Clinical Laboratory Improvements Amendments (CLIA). Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462, 82,554 (Dec. 28, 2000) (codified at 45 C.F.R. § 164.524).

99. *See* discussion *infra* Part III.D.

100. See 45 C.F.R. § 164.502 for a discussion of the general rules concerning uses and disclosures.

1. *Background: The Retreat from Consent and Expansion of the Notice Requirement*

The proposed Privacy Rule would have imposed the requirement of both consent and notice on covered entities.[101] Covered entities, particularly health care providers, would have been required to obtain consent and give notice prior to providing any care or treatment to a patient, and prior to processing claims in any manner.[102] The notice requirement, which survived in the final Rule in an expanded form, requires that a patient be provided with a written notice of privacy practices prior to the first treatment or payment encounter of uses and disclosures of protected health information for which consent or authorization are not required.[103] Consent is not required for uses and disclosures for treatment, payment, and health care operations.[104]

The consent requirement raised great concerns in the health care industry. As the Preamble to the final Privacy Rule somewhat dismissively stated:

> The issue that drew the most comments overall is the question of when individuals' permission should be obtained prior to use or disclosure of their health information. We learned that individuals' views and the legal view of "consent" for use and disclosure of health information are different and in many ways incompatible. Comments from individuals revealed a common belief that, today, people must be asked permission for each and every release of their health information. Many believe that they "own" the health records about them. However, current law and practice do not support this view.[105]

The practical problems of obtaining notice before *any* treatment or payment activity takes place were viewed as significant enough to eliminate the consent requirement. As the OCR has stated:

---

101. *See* Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462, 82,472–82,473 (Dec. 3, 2002) (to be codified at 45 C.F.R. pts. 160 and 164) (discussing the need to balance the competing interest of patient privacy and the current systems used by covered entities, the fact that the current systems used by covered entities show partial support for individuals' expectation of privacy and patients' expectations about their privacy rights all weigh in favor of consent and notice requirements).

102. *Id.*

103. *See* 45 C.F.R. § 164.520(a)(1) (stating that "an individual has a right to adequate notice of the uses and disclosers of protected health information that may be made by the covered entity, and of the individual's rights and of the covered entity's legal duties with respect to protected health information").

104. *Id.* § 164.506(a)(2). Consent is permitted, but not mandatory. *See id.* § 164.506(b).

105. Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462, 82,472 (Dec. 28, 2000) (codified at 45 C.F.R. §§ 160.101-164.534).

> The consent requirement created the unintended effect of preventing health care providers from providing timely, quality health care to individuals in a variety of circumstances. The most troubling and pervasive problem was that health care providers would not have been able to use or disclose protected health information for treatment, payment, or health care operations purposes prior to the initial face-to-face encounter with the patient, which is routinely done to provide timely access to quality health care.[106]

Examples of the "unintended effects" of the stringent notice requirement included pharmacists who would not have been able to fill a prescription, determine eligibility, or verify insurance coverage before the individual arrived at the pharmacy to pick up the prescription, if there was no prior consent.[107] Emergency medical providers were concerned that, even if a situation was urgent, they would have had to try to obtain consent to comply with the Privacy Rule, even if doing so would have been inconsistent with the "appropriate practice of emergency medicine."[108]

2. *The Final Federal Privacy Rule's Requirement of Notice and Acknowledgment*

Accordingly, in the final Privacy Rule, mandatory consent was replaced with a voluntary consent provision.[109] Further, the final Privacy Rule imposes on providers a requirement that a written notice be provided by all covered entities, and that health care providers obtain an acknowledgment of the notice (or document why they were not successful in doing so).[110] Under the final Privacy Rule, covered entities continue to be required to provide notice of all uses and disclosures for which consent and authorization are not required, including disclosures for treatment, payment, and health care operations.[111] Other examples include uses and disclosures required by law and disclosures for public health activities.[112]

The OCR has touted the notice requirement as an "opportunity to engage in important discussions regarding the use and disclosure of their health

---

106. Dec. 3, 2002 Guidance, *supra* note 1, at 8.
107. *Id.* at 7.
108. *Id.*
109. 45 C.F.R. § 164.506(b).
110. *Id.* § 164.520(c)(2)(i)-(ii).
111. *Id.* § 164.520(a)(1).
112. *Id.* § 164.512(a)-(b). Other uses and disclosures without consent or authorization are listed at section 164.512(c)-(k).

information."[113] This is optimistic at best, given the one-time notice requirement,[114] which as a practical matter will typically be administered by a clerk who will present the notice to the patient while the patient is waiting to be processed (and who typically is given an array of forms to read and sign) or provided as part of the enrollment process in a group health plan. Further, the requirements of the acknowledgment are minimal—all a patient or a personal representative has to do is acknowledge receipt, not that he or she understands the notice.[115] As discussed below, it is not clear whether this process affords the required or expected protection of privacy to uses and disclosures.[116] Most importantly, it is possible that the patient, and perhaps the public at large, may perceive that this cursory process does not protect their health information in the manner originally promised by the Act.

3. *Disclosures Pursuant to Authorization*

The Privacy Rule requires a HIPAA compliant authorization for the disclosure by covered entities to third parties.[117] This would include a covered disclosure of protected health information to employers, except to the extent the employer is fulfilling a health plan function.[118] It would also include disclosures to schools in many instances, which are specifically excepted out of the definition of "covered entities."[119] An authorization must also be used for disclosures of psychotherapy notes[120] and for marketing purposes.[121]

By all logic, disclosures by authorization should include disclosures to attorneys in the litigation context, continuing a practice codified in many states by statute.[122] However, the drafters of the Privacy Rule added some uncertainty

---

113. Dec. 3, 2002 Guidance, *supra* note 1, at 8.

114. 45 C.F.R. § 164.520(c)(1). For health plans, there is a requirement that once every three years employees be informed of the availability of the notice and how to obtain the notice. *Id.* § 164.520(c)(1)(ii).

115. *Id.* § 164.520(c)(2)(ii).

116. *See* discussion *infra* Part V.

117. 45 C.F.R. § 164.508. Section 164.508 requires an authorization in all cases except as "otherwise permitted or required by" part 164 of the Privacy Rule. *Id.* The core elements of the authorization are dictated by the Privacy Rule itself. *See id.* § 164.508(c)(1).

118. *Id.* § 164.502(e); Dec. 3, 2002 Guidance, *supra* note 1, at 41-42; *see also* discussion *infra* Part IV.

119. 45 C.F.R. § 164.508(c)(1).

120. See *supra* note 98 for a definition of psychotherapy notes.

121. *See* 45 C.F.R. § 164.508(a)(3)(i)-(ii). See *infra* Part IV.F for an extended discussion of marketing in the context of health plans.

122. *See, e.g.*, ARIZ. REV. STAT. § 12-2235 (2001) (requiring consent from patient before disclosure can be made in a civil action); COLO. REV. STAT. § 13-90-107 (2002) (providing that a physician may not testify without patient consent); IOWA CODE § 622.10(3) (2003) (setting out

to this practice by including a provision that specifically permits disclosure in judicial and administrative proceedings without consent or authorization, if certain conditions are met.[123] A close examination of that provision, however, makes it clear that the provision is generally more appropriate where the party whose information is being sought is not a party to the proceedings. However, the drafters did state: "The provisions in this paragraph [section 164.512(e)] are not intended to disrupt current practice whereby an individual who is a party to a proceeding and has put his or her medical condition at issue will not prevail without consenting to the production of his or her protected health information."[124] Accordingly, in cases where the patient is a party, an authorization that is consistent with both the Act and state law should protect covered entities in such disclosures.

4. *Disclosures of De-Identified Information*

The Privacy Rule recognizes that in some cases, health information may be needed or used that does not need to be "individually identifiable."[125] As discussed below, de-identified information may be useful in certain transactions involving employer health plans.

The Privacy Rule provides that information is not individually identifiable if it does not identify the individual or if the covered entity has no reasonable basis to believe it can be used to identify the individual.[126] The Privacy Rule provides two ways in which a covered entity can demonstrate that it has met the standard:

> One way a covered entity may demonstrate that it has met the standard is if a person with appropriate knowledge and experience applying generally accepted statistical and scientific principles and methods for rendering

---

procedures for obtaining consent or authorization to disclose medical information in the context of litigation).

123. 45 C.F.R. § 164.512(e). The Privacy Rule also provides that protected health information may be obtained in judicial and administrative proceedings with a court order or subpoena. *Id.* § 164.512(e)(1)(i)-(ii). However, section 164.512(e)(1)(ii) provides that a subpoena is only valid when the provider or other entity covered by the Privacy Rule receives "satisfactory assurance" that the party seeking the records has made a "good faith attempt" to give written notice to the patient whose records are being sought (or to mail notice to the patient's last known address). *Id.* § 164.512(e)(1)(ii). A literal reading of the Privacy Rule results in the conclusion that service of a subpoena on counsel for the patient as required by federal and state rules of civil procedure may not be sufficient to fulfill this requirement, which would make the use of a subpoena impracticable.

124. Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,530 (Dec. 28, 2000) (codified at 45 C.F.R. § 164.512(e)).

125. 45 C.F.R. § 164.514(a)-(b).

126. *Id.* § 164.514(a).

> information not individually identifiable makes a determination that the risk is very small that the information could be used, either by itself or in combination with other available information, by anticipated recipients to identify a subject of the information. The covered entity must also document the analysis and results that justify the determination. We provide guidance regarding this standard in our responses to the comments we received on this provision.[127]

In the alternative, a covered entity may use such information if it removes an entire list of enumerated identifiers and determines that it has no actual knowledge that the information could be used alone or in combination to identify a subject of the information.[128] The list of enumerated identifiers is extremely broad and includes name, all geographic identifiers other than state, date of birth, telephone numbers, e-mail, social security numbers, vehicle identifiers, and license numbers.[129]

C. *The Interrelationship of HIPAA and State Privacy Law: HIPAA Preemption*

1. *Introduction to HIPAA Federal Preemption of State Law*

The doctrine of federal preemption is based on the Supremacy Clause of the United States Constitution.[130] As the United States Supreme Court has explained, "the Constitution and laws passed pursuant to it are as much laws in the States as laws passed by the state legislature."[131] Further, as the Court stated in *Rose v. Arkansas State Police*,[132] "the Supremacy Clause invalidates all state laws that conflict or interfere with an Act of Congress."[133] Consequently, when a state law conflicts or interferes with a federal law, that state law is preempted by

---

127. Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. at 82,543.

128. *Id.* at 82,542-82,543.

129. 45 C.F.R. § 164.514(b).

130. *See* U.S. CONST. art. VI, § 1, cl. 2. The Supremacy Clause provides:

> This Constitution, and the laws of the United States which shall be made in Pursuance thereof; and all Treaties made, or which shall be made, under the Authority of the United States, shall be the supreme Law of the Land; and the Judges in every State shall be bound thereby, any Thing in the Constitution or Laws of any State to the Contrary notwithstanding.

Id.

131. Howlett v. Rose, 496 U.S. 356, 367 (1990).

132. Rose v. Ark. State Police, 479 U.S. 1 (1986).

133. *Id.* at 3.

the federal law. The principle equally applies to federal rules: any state law that is contrary to a federal rule is similarly preempted.[134]

The Act's federal preemption rule simply states that "[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."[135] However, the Privacy Rule becomes difficult to apply due to four exceptions.

The first preemption exception removes from federal preemption those state laws that the Secretary determines not to be preempted.[136] The Secretary, through his or her chief elected official or designee, reviews submissions from the state, and then makes a determination regarding whether the state law is preempted.[137]

The other exceptions to the general preemption rule include: (1) a "[s]tate law [that] requires a health plan to report, or to provide access to, information for the purpose of management audits, financial audits, program monitoring and evaluation, or the licensure or certification of facilities or individuals";[138] (2) state procedures for reporting "disease or injury, child abuse, birth, or death, or for the conduct of public health surveillance, investigation, or intervention";[139] and, most significantly, (3) state laws that relate to individually identifiable health information and are "more stringent" than the Act's Privacy Rule.[140]

---

134. *See generally* New York v. Fed. Energy Regulatory Comm'n, 535 U.S. 1, 18 (2002) (noting that a federal agency may preempt state law when it acts within its delegated authority).

135. 45 C.F.R. § 160.203 (2002).

136. In order to exempt a state law from federal HIPAA preemption, the Secretary must determine that the state law is necessary:

> (i) To prevent fraud and abuse related to the provision of or payment for health care;
> (ii) To ensure appropriate State regulation of insurance and health plans to the extent authorized by statute or regulation;
> (iii) For state reporting on health care delivery or costs; or
> (iv) For purposes of serving a compelling need related to public health, safety, or welfare, and, if a standard, requirement, or implementation specification under part 164 of this subchapter is at issue, as the Secretary determines that the intrusion into privacy is warranted when balancing against the need to be served; or
> (2) Has as its principle purpose the regulation of the manufacture, registration, distribution, dispensing, or other control of any controlled substances . . . or that is deemed a controlled substance by State law.

Id. § 160.203(a).

137. *Id.* § 160.204(a). For information on what must be included in the request, see *id.* § 160.204(a)(1)–(6).

138. *Id.* § 160.203(d).

139. *Id.* § 160.203(c).

140. *Id.* § 160.203(b); *see also id.* § 160.202 (defining "more stringent").

The analysis of whether a state law is preempted by the Act's Privacy Rule generally consists of a two-prong approach.[141] The first issue is whether the state law is contrary to the Privacy Rule.[142] In comparing the state law and the Privacy Rule, a provision is contrary when "(1) [a] covered entity would find it impossible to comply with both the State and federal requirements; or (2) [t]he provision of State law stands as an obstacle to the accomplishment and execution of the full purposes and objectives of [the Privacy Rule]."[143]

If a state law is contrary, then the next step of the analysis is to determine whether any of the state law exceptions apply.[144] Did the Secretary make a determination that the provision of state law is not preempted?[145] Does the state law provide for the reporting of disease or injury, child abuse, birth or death, or for the conduct of public health surveillance, investigation, or intervention?[146] Does the provision of state law require a health plan to report or provide access to information for the purpose of audits, monitoring and evaluation, or licensure?[147] Or is the provision in the state law more stringent regarding the privacy of individually identifiable health information than the Privacy Rule?[148]

Whether a state law is "more stringent" requires a detailed comparison of the state law with the Privacy Rule. "More stringent" is defined as a state law that (i) provides greater rights of access or amendment to the individual who is the subject of the individually identifiable health information; (ii) provides that same individual greater amount of information about use, disclosure, rights, and remedies; (iii) requires expressed legal permission from an individual before disclosure and "provides requirements that narrow the scope or duration, increase the privacy protections afforded . . ., or reduce the coercive effect of the circumstances surrounding the expressed legal permission"; or (iv) provides for more detailed information or a longer time period of record keeping regarding disclosures.[149] In addition, there is a catch-all provision which states that any

---

141. *See* Stewart v. La. Clinic, No. 99-1767, 2002 WL 31819130, at *3 (E.D. La. Dec. 12, 2002) (performing a preemption analysis to determine whether the state law was contrary to the Act or other federal law, and whether it fell under any of the state law exceptions).

142. *See id.*

143. 45 C.F.R. § 160.202.

144. *See* Stewart v. La. Clinic, 2002 WL 31819130, at *3 (examining the exception contained in 45 C.F.R. § 160.203(b)).

145. *See* 45 C.F.R. § 160.203(a).

146. *See id.* § 160.203(c).

147. *See id.* § 160.203(d).

148. *See id.* § 160.203(b).

149. *Id.* § 160.202. There is one other provision, which provides that state law is more stringent if it restricts the use or disclosure of protected health information that would otherwise be permitted, unless the disclosure is required by the Secretary in connection with determining

state law providing "greater privacy protection for the individual who is the subject of the individually identifiable health information" constitutes a "more stringent" state law.[150]

2. Stewart v. Louisiana Clinic[151]

The issue of whether the Act preempts a given state law can be complex. Understandably, there is not an abundance of case law on the subject, nor is it anticipated that there soon will be, as the Privacy Rule regarding preemption does not go into effect until April 14, 2003.[152] However, there is already one case, *Stewart v. Louisiana Clinic*, which reviewed preemption issues even before the Privacy Rule's implementation date.[153] The United States District Court's analysis in *Stewart* may shed light on how the Act's preemption issue will be handled by other courts.

The *Stewart* case involved a *qui tam* action where the United States chose not to intervene in the plaintiff's suit against the defendants who allegedly defrauded the federal government by submitting false claims for reimbursement for medical services provided to Medicare and Medicaid patients.[154] The defendants, which included a medical clinic and five doctors, argued that if they were compelled to produce medical records with individually identifiable health information, they could incur civil liability to the nonparty patients under the Louisiana law for disclosure of medical information.[155] The defendants asserted that the Louisiana health care statutes were not preempted by the Act.[156]

The court applied the Privacy Rules in this case for two reasons: (1) "'Although not presently binding . . . these regulations . . . [are] persuasive in that they demonstrate a strong federal policy of protection for patient medical records'";[157] and (2) the Privacy Rule will require full compliance when the case goes to trial (October 2003).[158] The court in this case focused on the issue of

---

whether a covered entity is abiding by the Privacy Rule or information to the individual who is the subject of the disclosure. *See id.*

150. *Id.*

151. Stewart v. La. Clinic, No. 99-1767, 2002 WL 31819130, at *1 (E.D. La. Dec. 12, 2002).

152. *See id.* at *2-3 (stating that the case is addressing a question of first impression, and noting that full compliance with the regulations is not required until April 14, 2003).

153. *Id.* at *3.

154. *See id.* at *1.

155. *Id.*

156. *Id.*

157. *Id.* at *3 (quoting United States v. Sutherland, 143 F. Supp. 2d 609, 612 (W.D. Va. 2001)).

158. *Id.*

whether the state law was contrary to the Act, and whether it fell under one of the exceptions, namely the exception for a more stringent state law that relates to privacy of individually identifiable health information.[159]

The defendants argued that the Act's disclosure requirements were less stringent than Louisiana law, which required "notice to the patient and a contradictory hearing that includes the patient before a health care provider can produce nonparty patient records without the patient's consent."[160] The Privacy Rule provides for disclosures without written authorizations or the opportunity for the patient to agree or object during a judicial proceeding under certain situations.[161]

The court stated that to fall under the "more stringent" exception, "[the] Louisiana law must (1) be 'contrary' to HIPAA or its Standards, (2) relate to the privacy of individually identifiable health information *and* (3) be 'more stringent' than federal law."[162] The court defined "more stringent" consistently with the Act's definition, meaning a state law that meets one or more of the following criteria:

> (4) with respect to the form, substance, or the need for express legal permission from an individual, who is the subject of the individually identifiable health information, for use or disclosure of individually identifiable health information, provides requirements that narrow the scope or duration, increase the privacy protections afforded . . . or reduce the coercive effect of the circumstances surrounding the expressed legal permission, as applicable.[163]

The defendants argued that the Louisiana law was more stringent than the Act's disclosure laws because Louisiana law requires patient consent of the individual, or in the alternative, Louisiana law provides that a "'court shall issue an order for the production and disclosure of a patient's records . . . only: after a contradictory hearing with the patient . . . and after finding by the court that the release of the requested information is proper.'"[164]

The court rejected the defendants' argument because "'the form, substance, or the need for express legal permission from an individual'" was not addressed in the Louisiana statute.[165] The Louisiana statute required the patient's consent

---

159. *See id.* (examining the exception contained in 45 C.F.R. § 160.203(b) (2002)).
160. *Id.*
161. *See* 45 C.F.R. § 164.512(e).
162. Stewart v. La. Clinic, 2002 WL 31819130, at *4.
163. *Id.* at *5 (citing 45 C.F.R. § 160.202).
164. *Id.* (quoting LA. REV. STAT. § 13:3715.1(B)(5)).
165. *Id.* (quoting 45 C.F.R. § 160.202) (emphasis omitted).

or a contradictory hearing with the patient, coupled with a finding by the court that the release of the requested information was proper.[166] Thus, the court concluded that the Louisiana statute did not fall within the "more stringent" exception to the Act's federal preemption rule.[167]

The court found in *Stewart* that both parties complied with the Privacy Rule by seeking a protective order from the court before the disclosure of nonparty patient health information.[168] Further, the court found that there was good cause for a protective order concerning nonparty patients' confidential medical records, and that the order should comply with section 164.512(e)(1)(v) of the Code of Federal Regulations.[169] The court's protective order required a two-fold production of nonparty patients' records, one of which was redacted, and one of which was not.[170] The plaintiffs were allowed to see the patients' names so that they could contact those patients and discuss with them the validity of their Medicare and Medicaid claims.[171] However, the protective order restricted the information to "counsel of record, no more than two paralegals . . . and one expert per party."[172] Finally, the court ordered that a confidentiality statement be attached to the disclosed records of nonparty patients that allowed disclosure of individually identifiable health information only for the purposes of the litigation, prescribed to whom the disclosures may be made, and required that all persons who received disclosed health information sign an affidavit agreeing to the terms of the protective order.[173] The *Stewart* case, despite being a precompliance deadline case, provides an example of how the preemption analysis may be utilized in future cases.

3. *State Preemption Analysis*

Because of the scope of the Act's preemption, a state-by-state analysis should be conducted showing which state laws are preempted and which are not. This Part focuses on Iowa's preemption initiative.

a. *Iowa HIPAA Preemption Workgroup and Preemption Analysis of Iowa Statutory Law.* A comprehensive analysis of each Iowa state statute and

---

166. *Id.*
167. *Id.*
168. *Id.*
169. *Id.* (referring to 45 C.F.R. § 164.512(e)(1)(v) and stating that a qualified protective order prohibits parties from using the information for any purpose other than litigation or a court proceeding and requires that it be returned or destroyed at the end of the litigation or proceeding).
170. *Id.* at *6, *9.
171. *Id.* at *6.
172. *Id.*
173. *Id.*

administrative code provision would require more time and space than available in the preemption portion of this Article. However, the Iowa Preemption Workgroup, consisting of representatives from the Iowa Medical Society, the Iowa Hospital Association, the Iowa State Bar Association, and the University of Iowa Hospitals and Clinics, analyzed the Iowa Code and designated certain enumerated statutes as preempted, partially preempted, or not preempted by the Act.[174] In addition, there are separate lists of Iowa laws that the Preemption Workgroup recommends for Department of Health and Human Services clarification or exception, and Iowa laws that the Preemption Workgroup recommends the Iowa Legislature consider for amendment.[175] The published statutory review, titled *Iowa HIPAA Preemption Analysis: A Report on the Relationship Between HIPAA's Privacy Rule and Iowa Statutory Law*, can be found at the Iowa Strategic National Implementation Process website.[176] Further, it is anticipated that the Iowa Preemption Workgroup will publish a similar review analyzing the Iowa Administrative Code.

The Preemption Workgroup's statutory review includes fifty-six subject areas, and discusses eight Iowa statutes that are preempted or partially preempted by the Act's Privacy Rule.[177] The Preemption Workgroup's list of Iowa statutes which are preempted or partially preempted includes: (1) "Iowa Code section 135.40-.42, Morbidity and Mortality/Quality Assurance Data"; (2) "Iowa Code section 147.135, Peer Review Committees"; (3) "Iowa Code section 228.3, Voluntary Disclosure of Mental Health Information"; (4) "Iowa Code section 228.9, Disclosure of Psychological Test Material"; (5) "Iowa Code section 229.25, Hospitalization of Persons with Mental Illness—Medical Records/Confidential/Exceptions"; (6) "Iowa Code section 235B.3, Dependent Adult Abuse Reporting/Investigation"; (7) "Iowa Code section 514B.30, Health Maintenance Organizations (HMO)—Confidential Communications"; and (8)

---

174. *See Iowa HIPAA Preemption Analysis: A Report on the Relationship Between HIPAA's Privacy Rule and Iowa Statutory Law* (2003), *at* www.iowasnip.org [hereinafter *Iowa HIPAA Preemption Analysis*]; *see also* STRATEGIC NAT'L IMPLEMENTATION PROCESS, AFFILIATE LISTINGS, *at* http://www.wedi.org/snip/public/articles/details%7E13.htm (last visited Mar. 3, 2003) (providing a list of HIPAA compliance efforts of the following states: Alabama, Arkansas, Colorado, Connecticut, District of Columbia, Delaware (tentative), Florida, Georgia, Idaho, Indiana, Kentucky, Louisiana, Massachusetts, Maryland, Maine, Michigan, Missouri, Mississippi, North Carolina, North Dakota, Nebraska, New Hampshire, New Jersey, New Mexico, Ohio, Oklahoma, Pennsylvania, Rhode Island, South Carolina, Tennessee, Texas, Utah, Virginia, Vermont, Wisconsin, and West Virginia (tentative)).

175. *See Iowa HIPAA Preemption Analysis*, *supra* note 174, at x-xi.

176. *See id.*

177. *See id.* at ix-x.

"Iowa Code section 141A.9(1)(l), Confidentiality of HIV/AIDS Information/Release to Employer."[178]

b. *How the Analysis Works: Communicable and Infectious Disease Reports Required by Law and Mental Health Disclosures of Psychological Test Material.* The following is an example of the statutory analysis of a non-preempted statute and a preempted statute.

i. *Communicable and Infectious Disease Reports Required by Law.* Iowa Code Chapter 139A, entitled "Communicable and Infectious Diseases and Poisonings," requires reports be filed with the Iowa Department of Health.[179] The first prong: Is the Iowa law contrary to the Privacy Rule? Reports required under Iowa Code Chapter 139A comply with the Privacy Rule, which allows a covered entity to disclose protected health information for public health activities by a "public health authority authorized by law to collect or receive such information for the purpose of preventing or controlling disease . . . including . . . the reporting of disease."[180] Thus, the Iowa laws on reporting communicable or infectious disease are not preempted because they are not contrary to the Privacy Rule.[181]

The Iowa law protects the patient's privacy by stating that "[a] report to the department, to a local board, or to a local department, which identifies a person infected with a reportable disease, is confidential and shall not be accessible to the public."[182] Under Iowa law, "[a]ny person who, acting reasonably and in good faith, files a report under this section is immune from any liability, civil or criminal, which might otherwise be incurred or imposed for making a report."[183]

For a practical example, if a covered entity receives a report questionnaire from the Iowa State Health Registry regarding a cancer patient, the covered entity must still file the report. Cancer is listed as a reportable disease,[184] and the Iowa Department of Public Health has appointed the State Health Registry to compile that information.[185]

---

178. *Id.*

179. IOWA CODE § 139A.3(1) (2003).

180. 45 C.F.R. § 164.512(b) (2002).

181. Even if the Iowa Chapter 139A laws *were* contrary to the Federal Rule, the analysis would lead one to look for an exception under 45 C.F.R. section 160.203. In particular, 45 C.F.R. section 160.203(c), allowing an exception for state laws that provide for the reporting of diseases, appears to be applicable. *See also Iowa HIPAA Preemption Analysis*, *supra* note 174, at 7.

182. IOWA CODE § 139A.3(2)(b).

183. *Id.* § 139A.3(2)(a).

184. IOWA ADMIN. CODE r. 641-1.3(1)(b) (2001).

185. *Id.* r. 641-1.3 n.***.

ii. *Mental Health Disclosures of Psychological Test Material.* A general description of what mental health information may be disclosed, and to whom it may be disclosed, is found in Iowa Code Chapter 228.[186] Generally, the Iowa mental health disclosure laws are not contrary or are more stringent, thus state law should continue to be followed and where not contrary, both state law and the Act should be followed.[187]

That being said, the Act *does* preempt Iowa law regarding disclosures of psychological test material to the patient/subject of the testing.[188] Section 228.9 of the Iowa Code prevents the disclosure of psychological test material to any person, including the test subject, in any administrative, judicial, or legislative proceeding, except where explicitly allowed in the section.[189] Currently, under Iowa law, an individual may have his or her psychological test material sent to a designated licensed psychologist to whom the test materials may be disclosed, but the individual does not have a right to inspect the materials.[190]

The first prong: Is Iowa Code section 228.9 contrary to the Act? Iowa Code section 228.9 is contrary to the Act's privacy rules on the patient's right to access their own protected health information. The Privacy Rule states that an individual cannot be denied access to their own protected health information unless that person is reasonably likely to endanger their own physical safety or that of another.[191] The federal privacy rules would allow a test subject access to their psychological test materials so long as they were not reasonably likely to endanger their own physical safety or that of another.[192] The Iowa law is contrary to the Privacy Rule because, under the Iowa law, the individual is prevented from receiving the test materials even if they are not reasonably likely to endanger their own or another's physical safety.[193]

---

186. *See generally* IOWA CODE ch. 228.

187. *Iowa HIPAA Preemption Analysis*, *supra* note 174, at 27-33.

188. *See* 45 C.F.R. § 160.203(c) (preempting conflicting state law unless the state law meets certain requirements); *Iowa HIPAA Preemption Analysis*, *supra* note 174, at 27-33 (examining disclosure of mental health records under Iowa law and its interaction with the Act's preemption rule); *see also infra* text accompanying notes 189-93. In addition, the Iowa Workgroup states that a covered entity should "[f]ollow HIPAA where a person who is a 'legal representative' under state law is not a 'personal representative' under HIPAA." *Iowa HIPAA Preemption Analysis*, *supra* note 174, at 28.

189. IOWA CODE § 228.9.

190. *Id.*

191. 45 C.F.R. § 164.524(a), (a)(2)(ii), (a)(3)(i); *see also Iowa HIPAA Preemption Analysis*, *supra* note 174, at 33.

192. *See* 45 C.F.R. § 164.524(a).

193. *See* IOWA CODE § 228.9.

The second prong: Does the *contrary* Iowa law fall into one of the exceptions under 45 C.F.R. section 160.203. No exception exists.[194] As such, the Privacy Rule preempts state law in this context.

The above analysis illustrates the fact that the preemption principles of the Act make it a difficult rule to apply given the broad range of longstanding state laws and practices. Further, in states where there is no formal preemption analysis, covered entities may be left to guess as to which law applies.

D. *Patient Rights*

The Privacy Rule provides patients with a number of rights in regard to personal health information. In addition to the right of adequate notice,[195] a patient has the right of access to his or her protected health information,[196] the right to seek amendment of protected health information,[197] and the right to an accounting.[198] A patient also has a right to restrict the dissemination of his or her health information by limiting the individuals or entities to which information may be disclosed,[199] and further has the right to limit the time and place of disclosure.[200] Many of these rights may have already existed either as a matter of law or practice, but the Act requires covered entities to establish protocols for patients to exercise these rights,[201] imposing on covered entities what may prove to be a substantial administrative burden. The right of access, the right to seek an accounting, and the right to request an amendment are discussed in detail here. These and other individual rights are discussed in the context of the patient scenario.

1. *The Right of Access*

Under the Privacy Rule, a patient has a right of access to "inspect and obtain a copy of protected health information about the individual in a designated record set."[202] A covered entity has a right to deny access in very limited circumstances, including where:

---

194. *See* 45 C.F.R. § 160.203(a)-(d).
195. *Id.* § 164.520.
196. *Id.* § 164.524.
197. *Id.* § 164.526.
198. *Id.* § 164.528.
199. *Id.* § 164.522.
200. *Id.* § 164.524(c)(3).
201. *Id.* § 164.530.
202. *Id.* § 164.524(a)(1).

> [a] licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person; [or] [t]he protected health information contains references to another person . . . and a licensed health care professional has determined . . . that the access requested is reasonably likely to cause substantial harm to such other person.[203]

Patients have long had the right of access to their medical information outside the confines of the Act.[204] The right of access under the Act is not as broad as it seems, as the right is limited to the designated record set, which is not entirely coextensive with the medical record; notably, it excludes psychotherapy notes.[205] Further, the right is somewhat confusing in its limitations. If a patient requests a copy of records for transfer of care, the records provided to the patient should not be limited to the scope of the designated record set in order to ensure continuity of quality care.

2. *The Right to an Accounting*

An individual has a right to receive an accounting of disclosures of protected information made by the covered entity for the six years preceding the request.[206] The Privacy Rule does not limit the number of requests a patient may make in a year, but only the first one is free; after that, the entity may charge a fee for the service.[207] Again, the right would appear broader than it is. However, perhaps recognizing potential administrative burdens, the right to an accounting does not include disclosures for treatment, payment, and health care operations.[208] It also does not include disclosures made as required by law, or pursuant to an authorization.[209] Nevertheless, covered entities must have procedures or technology in place to track all other disclosures and to generate accountings as requested.[210]

---

203. *Id.* § 164.524(a)(3)(i)-(ii).

204. *See* A. Craig Eddy, *A Critical Analysis of Health and Human Services' Proposed Health Privacy Regulations in Light of the Health Insurance Privacy and Accountability Act of 1996*, 9 ANNALS HEALTH L. 1, 4 (2000) (indicating that after World War II, medical paternalism declined and patients were given access to their own medical information).

205. *See* Hughes, *supra* note 95; *see also* discussion *supra* Part III.A.6.

206. 45 C.F.R. § 164.528(a)(1).

207. *Id.* § 164.528(c)(2).

208. *Id.* § 164.528(a)(1)(i).

209. *Id.* § 164.528(a)(1)(ii), (iv)-(v).

210. *Id.*; *see also id.* § 164.530(f)(i)(1).

3. *The Right to Seek an Amendment*

The Privacy Rule includes a right to seek amendment of protected health information.[211] The Privacy Rule states that "[a]n individual has the right to have a covered entity amend protected health information about the individual in a designated record set for as long as the protected health information is maintained in the designated record set."[212] The right itself is not absolute, as a covered entity has the right to deny a request for an amendment under certain circumstances.[213] These circumstances include: (1) if the record is not part of the designated record set; (2) if the information is accurate and complete; and (3) if the information was not created by the covered entity, unless there is a reason to believe the originator of the information is not available to act on the original amendment.[214] The entity must have in place policies and procedures for reviewing a request and must act on it within sixty days.[215] If an amendment is denied, the covered entity must permit the individual to submit to the covered entity a statement of disagreement.[216] A covered entity may submit a rebuttal statement.[217] The request, the statement of agreement, and the rebuttal must be "linked" to the designated record set, that is, placed with the designated record set.[218]

The right to seek an amendment is highly problematic. Although a covered entity may deny an amendment on the grounds that the information is "correct" and "complete,"[219] these criteria are difficult to apply, particularly if the amendment is to a diagnosis rather than to objective findings. In addition, to the extent that an individual's medical records play an important role in many kinds of lawsuits—from personal injury to medical negligence—it is possible that seeking an amendment of critical medical information may become a part of litigation strategy in certain cases.

---

211. *Id.* § 164.526.
212. *Id.* § 164.526(a)(1).
213. *Id.* § 164.526(a)(2).
214. *Id.*
215. *Id.* § 164.526(b)(2).
216. *Id.* § 164.526(d)(1).
217. *Id.*
218. *Id.*
219. *See id.* § 164.526(a)(2).

E. *Penalties and Enforcement*

The penalties for violations of the Privacy Rule are dictated by the Act.[220] For unintentional violations of a provision of the Privacy Rule, a single violation of any provision will result in a $100 fine.[221] Multiple violations of an identical requirement or of any prohibitions in the Privacy Rule, made during a calendar year may result in fines up to $25,000.[222] For willful disclosures of individually identifiable health information, the monetary penalties are up to $50,000, and such disclosures may result in a term of imprisonment of up to one year for any person committing the offense.[223] Willful disclosures of individually identifiable health information "committed under false pretenses" may result in monetary penalties of up to $100,000 and up to five years in prison for any person committing the offense.[224] Wrongful disclosures of individually identifiable health information committed under false pretenses with an intent to sell or use such information for commercial advantage, personal gain, or malicious harm may result in penalties of up to $250,000 and up to ten years in prison for any person committing the offense.[225]

Although the statutory penalties raised the specter of strict enforcement, the Department of Health and Human Services has let it be known that the enforcement climate for the Privacy Rule would be on fostering compliance rather than on penalizing noncompliance.[226] The OCR will enforce the Privacy Rule.[227] The OCR has stated that the enforcement process will be "complaint-driven."[228] The stated goal is to obtain voluntary compliance through technical assistance, which will give a violating covered entity the opportunity to undertake corrective action.[229]

IV. EMPLOYER HEALTH PLANS AND THE INSURANCE INDUSTRY—SELECTED ISSUES

While there has been much focus placed on the Act and its effect on health care providers, employers have been grappling with the Act and its impact on

---

220. HIPAA of 1996, Pub. L. No. 104–191, § 262, 110 Stat. 1936, 2028-29 (1996) (codified at 42 U.S.C. § 1320(d)(5)-(6) (2000)).
221. *Id.*
222. *Id.*
223. *Id.*
224. *Id.*
225. *Id.*
226. *See* Eddy, *supra* note 204, at 5.
227. *Id.* at 31.
228. *Id.* at 28.
229. *Id.* at 31.

human resources functions that use employees' protected health information. Under the Act, employer group health plans are defined as covered entities.[230] As a result, employers must become familiar with the Act and determine how to make their group health plans compliant. Since as many as nine out of ten Americans obtain their health coverage through their employers, this is a major task.[231] Most employers have another year, until April 14, 2004, to finalize their compliance plans with the Privacy Rule.[232] However, many of these employers have been asked to comply sooner, because third-party administrators and insured health plan providers must implement their compliance plans by the

---

230. 45 C.F.R. § 160.103 (2002). The regulations define a group health plan as follows:

> *Group health plan* (also see definition of *health plan* in this section) means an employee welfare benefit plan (as defined in section 3(1) of the Employee Retirement Income and Security Act of 1974 (ERISA), 29 U.S.C. 1002(1)), including insured and self-insured plans, to the extent that the plan provides medical care (as defined in section 2791(a)(2) of the Public Health Service Act (PHS Act), 42 U.S.C. 300gg-91(a)(2)), including items and services paid for as medical care, to employees or their dependents directly or through insurance, reimbursement, or otherwise, that:
>
> (1) Has 50 or more participants (as defined in section 3(7) of ERISA, 29 U.S.C. 1002(7)); or
>
> (2) Is administered by an entity other than the employer that established and maintains the plan.
>
> . . . .
>
> *Heath plan* means an individual or group plan that provides, or pays the cost of, medical care (as defined in section 2791(a)(2) of the PHS Act, 42 U.S.C. 300gg-91(a)(2)).
>
> (1) *Health plan* includes the following, singly or in combination:
>
> (i) A group health plan, as defined in this section. . . .
>
> (viii) An employee welfare benefit plan or any other arrangement that is established or maintained for the purpose of offering or providing health benefits to the employees of two or more employers.

Id. This Part will focus on health plans typically offered by a single employer, such as group health plans (fully and self-funded), flexible spending arrangements in the form of medical reimbursement arrangements, typically provided under a § 125 plan (commonly referred to as cafeteria plan) and health reimbursement arrangements under Internal Revenue Code § 105.

231. Cordone, *supra* note 12, at 196 (citing THE WHITE HOUSE DOMESTIC POLICY COUNCIL, HEALTH SECURITY: THE PRESIDENT'S REPORT TO THE AM. PEOPLE, 93 (1993)).

232. For group health plans that are covered by the Privacy Rule, there are two implementation dates, depending upon the size of the plan. Small health plans have until April 14, 2004 to comply with the Privacy Rule, while health plans other than small plans are required to comply by April 14, 2003. 45 C.F.R. § 164.534(b). The Privacy Rule defines a small health plan as "a health plan with receipts of $5 million or less." *See id.* There was some issue as to what receipts to use to make this determination, which was clarified by the recent OCR guidance. *See* Dec. 3, 2002 Guidance, *supra* note 1, at 110-11 (providing a link to the HHS website on small health plans at http://cms.hhs.gov/hippa/hipaa2/default.asp).

April 2003 deadline.[233] This Part examines some of the practical issues that employers who sponsor single-employer health plans must navigate in interacting with the insurance industry and in implementation of the Privacy Rule.

An employer becomes privy to employees' protected health information in a variety of ways, including: administration of workers' compensation claims, determining an employee's qualification for leave under the Family and Medical Leave Act, or assessing what reasonable accommodations might be made for an employee with a qualifying disability under the Americans with Disabilities Act. However, in none of these contexts is the employer an entity covered by the Act.[234]

Only in its capacity as a plan sponsor of a group health plan is an employer faced with complying with the Privacy Rule, thus leaving the burden of navigating the full scope of the Privacy Rule to those employers who sponsor self-funded plans.[235] The Privacy Rule provides that:

---

233. Health plans, which offer fully insured products to group plans, are required to comply by April 14, 2003. 45 C.F.R. § 164.534(b)(1). The authors' recent experience has been that health plans that also provide third party administration services are requiring their clients to amend their plans and sign business associate agreements without regard to plan size to meet the earlier compliance date. *See, e.g.*, WELLMARK, BLUECROSS BLUESHIELD, HIPAA-AS FOR SELF FUNDED GROUP HEALTH PLANS, *at* http://wellmark.com/hipaa/hipaa_groupSelf-funded.htm (2002).

234. Employers are not defined as covered entities under the Privacy Rule. *See* 45 C.F.R. § 160.103.

235. The Privacy Rule requires a plan sponsor to amend its group health plan and agree to comply with the amendment's provisions in order to receive protected health information from the plan. *Id.* § 164.504(f)(1)(i), (f)(2)(ii). A plan sponsor that receives only summary health information for the purposes of obtaining premium bids or modifying, amending, or terminating the group health plan, and participant enrollment information, does not have this compliance burden. *Id.* § 164.504(f)(1)(ii)-(iii). Additionally, group health plans that provide health benefits "solely through an insurance contract with a health insurer or HMO" and that receive only the summary health information described above, are not required to provide or maintain a privacy practices notice for the group health plan. *Id.* § 164.520(a)(2)(iii). As a result, employers with fully insured plans (i.e., group plans that obtain their insurance coverage for their participants from health plans (another covered entity under the Act)) do not have the full HIPAA compliance burden because the health insurance insurer is the HIPAA entity that has the full compliance burden. See *supra* Part III.A, B, D, and E for a full discussion on the compliance obligations of a covered entity. See also WELLMARK, BLUECROSS BLUESHIELD, HIPAA-AS FOR FULLY INSURED GROUP HEALTH PLANS, at http://welmark.com/hipaa/hipaa_groupFullyInsured.htm (2002), for an example of a health plan's compliance program for fully insured group health plan clients. The Privacy Rule defines a health insurance insurer to mean "an insurance company, insurance service, or insurance organization (including an HMO) that is licensed to engage in the business of insurance in a State and is subject to State law that regulates insurance. Such term does not include a group health plan." 45 C.F.R. § 160.103. An employer sponsoring a self-funded plan may transfer the plan's HIPAA compliance duties to a business associate, typically a third party administer. *See* discussion *infra* Part IV.E. However, the employer still retains the ultimate legal responsibility for compliance under the Privacy Rule. *See* discussion *infra* Part IV.E.

> A group health plan, in order to disclose protected health information to the plan sponsor or to provide for or permit the disclosure of protected health information to the plan sponsor by a health insurance issuer or HMO with respect to the group health plan, must ensure that the plan documents restrict the uses and disclosures of such information by the plan sponsor consistent with the requirements of this subpart.[236]

The only disclosure activity that is permitted by the Privacy Rule, absent a change to the plan's documents, is the disclosure of summary health information by the employer for the purpose of "[o]btaining premium bids from health plans for providing health insurance coverage under the group health plan."[237]

A. *HIPAA Group Health Plan Requirements*

The practical dilemma for an employer is that in administration of its group health plan, the employer typically does not think of the plan as an entity separate and distinct from the employer. The administration of most plans is done within the employer's human resources department. In the case of smaller employers, employees designated as human resources personnel may also have other, unrelated duties. However, because of the Act, the plan must be thought of as a separate entity with specific obligations under the Privacy Rule, and the employer's actions with regard to the health plan must be HIPAA compliant.[238]

While an employer is not defined as a covered entity under the Act, the Privacy Rule expands the Act's coverage to the employer through the requirement of a plan amendment that incorporates specific HIPAA provisions into a plan document, and the requirement of a certification by the employer of adherence to the contents of the amendment.[239] The plan amendment must contain the following elements:

---

236. 45 C.F.R. § 164.504(f)(1)(i).

237. *Id.* § 164.504(f)(1)(ii)(A). The Privacy Rule also permits a plan sponsor to disclose summary health information for the purpose of modifying, amending, or terminating the group health plan. *Id.* § 164.504(f)(1)(ii)(B). However, this exception is likely to be rarely used in practice because it is difficult to imagine a scenario where a plan sponsor would be disclosing summary health information to a third-party for the purpose of amending or terminating the plan (although underlying claims may be the impetus for the employer to amend the plan to address plan design issues and plan language ambiguities in the benefits covered).

238. For a practical discussion of the administration of a group health plan under the Act, see Amy Gordon & Kathy Schwappach, *How HIPAA Will Change Group Health Plan Administration*, J. OF PENSION BENEFITS, Autumn 2002, at 33-36.

239. 45 C.F.R. § 164.504(f)(2). There may be an issue of whether the Privacy Rule is overreaching and beyond the scope of the statute in its requirements of this amendment and certification process, because in practice these requirements impose many covered entity requirements on the plan sponsor. The issue is similar to the commentary on the concept of the

A. Permitted and required uses and disclosure of protected health information (PHI) that are consistent with the Privacy Rule;[240] and
B. Provisions that require the plan sponsor to take the following actions:

1. To not use or disclose PHI other than as permitted by the plan or by law;
2. To ensure that its agents, including subcontractors, to whom the plan sponsor provides PHI, agree to the same conditions and restrictions on disclosing PHI that apply to the plan sponsor (similar to business associates);
3. To not use or disclose the information in any other employment-related activity (including other benefit plan decisions);
4. To report to the plan (i.e., itself) any use or disclosure that is inconsistent with the plan's terms;
5. To make PHI available to a plan participant for inspection;
6. To make PHI available to a plan participant for amendment;
7. To make an accounting to a plan participant of PHI disclosures;
8. To make its internal practices, books, and records relating to the plan available to the Secretary for compliance purposes;
9. To return or destroy all PHI received from the plan when no longer needed for the disclosure, or to take steps to limit further use and disclosure; and
10. To provide for adequate separation between the plan and the plan sponsor-employer by (a) describing those employees or classes of employees or other persons under the employer's control that will have access to the plan PHI; (b) restricting the use and access to plan PHI to these individuals' plan administration functions; and (c) providing an effective mechanism to correct non-compliance issues with these individuals.[241]

---

business associate greatly expanding the reach of the Act by rulemaking. *See* discussion *supra* Part III.A.5. The OCR has not issued any statements defending the plan sponsor requirements to date.

240. 45 C.F.R. § 164.504(f)(2)(i).

241. *Id.* § 164.504(f)(2)(ii)-(iii).

The employer is then required to certify its HIPAA compliance before the plan is permitted to disclose PHI to the employer in its capacity as plan sponsor.[242]

While the employer may consider the written plan amendment and certification requirements merely as additional paperwork to manage for the health plan (and more documents for the insurance company or third-party administrator (TPA) to generate for the employer's use as the plan sponsor), the employer's compliance with these requirements means that the employer may conduct its business with the plan in a way similar to pre-HIPAA days. Employers need to pay close attention to the contents of the Act's plan amendments that are made to their health plans, especially amendments that will govern the Act's administration of a self-funded plan, because the employer in that case will ultimately be responsible to ensure the plan's compliance with the Privacy Rule.

Most employers will likely rely on the insurance company that has provided the insurance product for its fully insured plan to draft this amendment, or in the case of a self-funded plan, the TPA for the plan. A well-drafted amendment may greatly reduce the need for the plan to enter into business associate agreements because many of the services provided to a plan are, upon careful analysis, provided to the employer as the plan sponsor and not to the plan directly.

B. *The Insurance Professional's Relationship to the Plan*

In navigating the Act, it is critical for employers and their insurance professionals to focus on which entity—the health plan or the employer—is actually engaging the services of the insurance professionals (or any other service provider to the plan). In the case of most smaller, single-employer plans, it is the employer as the plan's sponsor, and not the plan itself, that uses the services of an insurance broker, contracts for stop loss coverage, or retains an attorney to assist in plan design or advise the employer on benefit disputes under the terms of the plan. In many cases, employers are the contracting party with the plan's TPA (although under the Act, this practice will likely change to ensure that the plan is the contracting entity, bound by the plan sponsor (the employer) as signatory to the TPA agreement). Beyond the TPA, the plan may have few additional business associates. The plan amendment, if drafted carefully to fully set forth the parties to whom the plan sponsor may disclose PHI in the course of

---

242. *See id.* § 164.504(f)(2)(ii) ("[T]he group health plan will disclose protected health information to the plan sponsor only upon receipt of a certification by the plan sponsor that the plan documents have been amended to incorporate the following provisions and that the plan sponsor agrees to [such provisions].").

its plan administration, could alleviate the need for a multitude of business associate agreements. Entities that provide plan services through the plan sponsor, rather than directly to the plan, would be able to access PHI through the employer if the amendment sets forth these uses and disclosures.

The role of the insurance broker in his or her relationship to the employer health plan may be used to illustrate the benefit of the amendment and certification requirement, and how the Act may change this relationship. Many employers are struggling with how to disclose PHI to brokers during the renewal process.[243] Are brokers business associates of the plan[244] or agents of the noncovered entity, the employer? The Privacy Rule can be interpreted to provide that if (1) a plan amendment is made that lists the disclosure of PHI by the employer to a broker or other entities for renewal purposes, and (2) the employer completes the necessary certification that the plan amendment has been made and the employer-plan sponsor agrees to comply, then the employer is permitted to use the PHI for renewal purposes.[245]

1. *Application of Minimum Necessary*

Disclosures from employers to brokers would still have to be consistent with the Privacy Rule, which would require that PHI be de-identified to the extent possible, because no exclusion from the minimum necessary rule exists for this type of disclosure.[246] If the underwriter requires participant specific PHI when assessing plan participants that have incurred high-dollar claims during the course of a plan year, the Act's minimum necessary concept would dictate that the plan strip the identifying information from the data. For example, providing redacted patient records, if required by the underwriter, and identifying all records associated with that particular participant with a neutral identifier (e.g., participant A).

---

243. As previously explained, the Privacy Rule does permit the plan to disclose PHI to the plan sponsor to obtain premium bids without a plan amendment. *See supra* text accompanying note 237. For purposes of this discussion, it is assumed the broker will be providing services beyond the scope of premium bids, which would require a plan amendment. *See id.*

244. See *supra* Part III.A.5 for a discussion of business associates.

245. *See* 45 C.F.R. § 164.504(f)(1)(ii)(A) ("The group health plan . . . may disclose summary health information to the plan sponsor, if the plan sponsor requests the summary health information for the purpose of . . . [o]btaining premium bids from health plans for providing health insurance coverage under the group health plan . . . ."); Dec. 3, 2002 Guidance, *supra* note 1, at 42 (listing exceptions to the business associate standard and including "disclosures to a health plan sponsor, such as an employer, by a group health plan . . . provided that the group health plan's documents have been amended to limit the disclosures or one of the exceptions at 45 C.F.R. § 164.504(f) have been met").

246. 45 C.F.R. § 164.502(b); *see also* discussion *supra* Parts III.A.4, III.B.4 (discussing the concept of minimum necessary and de-identified information).

In the December 3, 2002 Guidance, the OCR explained the concept of minimum necessary in this fashion:

> The HIPAA Privacy Rule requires a covered entity to make reasonable efforts to limit use, disclosure of, and requests for protected health information to the minimum necessary to accomplish the intended purpose. To allow covered entities the flexibility to address their unique circumstances, the Rule requires covered entities to make their own assessment of what protected health information is reasonably necessary for a particular purpose, given the characteristics of their business and workforce, and to implement policies and procedures accordingly. This is not an absolute standard and covered entities need not limit information uses or disclosures to those that are absolutely needed to serve the purpose. Rather, this is a reasonableness standard that calls for an approach consistent with the best practices and guidelines already used by many providers and plans today to limit the unnecessary sharing of medical information.
>
> The minimum necessary standard requires covered entities to evaluate their practices and enhance protections as needed to limit unnecessary or inappropriate access to protected health information. It is intended to reflect and be consistent with, not override, professional judgment and standards. Therefore, it is expected that covered entities will utilize the input of prudent professionals involved in health care activities when developing policies and procedures that appropriately limit access to personal health information without sacrificing the quality of health care.[247]

The Guidance contemplates that an entire medical record can be disclosed, provided that the covered entity's documents in its policies and procedures state that such disclosure is appropriate for the identified purpose.[248]

2. *Business Associate—Yes or No?*

If the employer maintains the relationship with the broker, the employer may wish to consider whether the employer enters into an agreement or letter of understanding with the broker on the use and disclosure of the PHI to comply with the Privacy Rule plan amendment requirement that any plan sponsor agent (in this case, the broker acting on behalf of the plan sponsor to obtain services for the plan and its participants) agree to the same restrictions that apply to the plan sponsor with regard to the health information.[249] Because the employer is not the

---

247. Dec. 3, 2002 Guidance, *supra* note 1, at 24.
248. *Id.* at 22.
249. 45 C.F.R. § 164.504(f)(2)(ii)(B).

covered entity, the agreement would not be a business associate agreement,[250] but may contain many of the same provisions found in such an agreement.

There is nothing to prohibit the plan from treating the broker as the plan's business associate and entering into a business associate agreement during the underwriting process. The minimum necessary concept must be followed by the plan's business associates.[251] If the broker is to be treated as a business associate, then the PHI received by the broker, and the uses and disclosures of the PHI by the broker, must be limited to be consistent with the plan's policies and procedures. This might be done as part of the business associate agreement,[252] either through a recitation within the contract of the applicable procedure or policies, or a wholesale approach of incorporating the policies and procedure by reference into the agreement between the parties.[253] Either approach would require some monitoring by the plan to ensure that the broker was provided the

---

250. *Id.* § 160.103.

251. Dec. 3, 2002 Guidance, *supra* note 1, at 28. The Guidance sets forth the following regarding the minimum necessary and the application of this standard to business associates:

> A covered entity's contract with a business associate may not authorize the business associate to use or further disclose the information in a manner that would violate the HIPAA Privacy Rule if done by the covered entity. Thus, a business associate contract must limit the business associate's uses and disclosures of, as well as requests for, protected health information to be consistent with the covered entity's minimum necessary policies and procedures. Given that a business associate contract must limit a business associate's requests for protected health information on behalf of a covered entity to that which is reasonably necessary to accomplish the intended purpose, a covered entity is permitted to reasonably rely on such requests from a business associate of another covered entity as the minimum necessary.

Id. (citations omitted).

252. See discussion *supra* Part III.A.5 for the basic HIPAA concept of business associate. As discussed in that Part, the revised Privacy Rule contains some transition rules with regard to when the written business associate contract is required to be in place between a covered entity and the business associate. *See* 45 C.F.R. § 164.532 (d), (e). Covered entities (other than small health plans) that have existing written contracts prior to October 15, 2002 are permitted to continue to operate under the existing agreement up to April 14, 2004 (which is the small plan compliance date), provided that the contract is not renewed or modified before April 14, 2003. *Id.* § 164.532(e). This extension is not an extension for the covered entity to delay compliance with the Act; rather, the covered entity must comply with the Privacy Rule in all other respects, including permissible disclosures to the business associate as required under the Privacy Rule. *See id.* § 165.504(e)(2)(i). With the continued HIPAA privacy obligations, in practice, it may be easier for the covered entity to ensure compliance by the business associate if the agreement is in place sooner. This extension does not apply to oral contracts. *See id.* § 165.532(d).

253. The model business associate contract provisions do not contain any sample sections that specifically address the minimum necessary concept. OCR, *supra* note 84; *see also* Dec. 3, 2002 Guidance, *supra* note 1, at 52 (stating that "a business associate contract must limit a business associate's uses and disclosures of, as well as requests for, protected health information to be consistent with the covered entity's minimum necessary policies and procedures").

most current policies and procedures, because the plan has the ultimate HIPAA liability for impermissible disclosures.[254]

C. *Stop Loss Coverage*

For a self-funded plan, renewal underwriting may occur when an employer procures stop loss coverage to cap the employer's exposure to high-dollar claims in the plan year.[255] Because this insurance is typically obtained by the employer to cover the risks associated with its self-funding of the plan, and not regular claims brought under the plan, care should be given not to make stop loss coverage a plan obligation, as this may impact the plan's ability to argue Employee Retirement Income Security Act of 1974 (ERISA) preemption and avail itself of the benefits of coverage under ERISA rather than state insurance laws.[256] The Privacy Rule does not treat the reinsurer as a business associate of

---

254. The business associate concept contemplates that the obligations to comply with the Privacy Rule are imposed upon the business associate by the covered entity and are contractual in nature, and not imposed by the Privacy Rule. Dec. 3, 2002 Guidance, *supra* note 1, at 44.

> Business Associates, however, are not subject to the requirements of the Privacy Rule, and the Secretary cannot impose civil monetary penalties on a business associate for breach of its business associate contract with the covered entity, unless the business associate is itself a covered entity. For example, covered entities do not need to ask their business associates to agree to appoint a privacy officer, or develop policies and procedures for use and disclosure of protected health information.

Id. A covered entity may consider drafting the contract to permit the covered entity to recoup any damages arising from HIPAA liability incurred by the covered entity and caused by the business associate, likely through some type of indemnification provision.

However, it should be noted that the covered entity is *not* required under the Privacy Rule to monitor its business associates' actions, and the covered entity is not liable for noncompliance by business associates, provided those steps outlined under the Privacy Rule are followed. *See id.* at 46 ("[C]overed entities are not required to monitor or oversee the means by which their business associate abides by the privacy requirement of the contract. Nor is the covered entity responsible or liable for the actions of its business associates."). These actions include taking reasonable steps to cure a material breach or violation of the parties' contract upon discovery by the covered entity, and termination of the contract by the covered entity if such actions are unsuccessful. 45 C.F.R. § 164.504(e)(1)(ii). If the contract cannot be terminated, then the covered entity must report to the Secretary. *Id.* § 164.504(c)(1)(ii)(B). A cure and termination provision that mirrors the Privacy Rule should be standard in any business associate agreement.

255. Typically, employers that sponsor self-insured plans will obtain insurance from an insurance company so as to provide coverage to the employer in the event claims under such a self-insured plan exceed a certain dollar amount during the course of the plan year. Employee Benefits Management, Stop Loss Insurance CCH § 10,355 (2002). Stop loss insurance is usually designed to pay if claims reach a specific (claims over a certain dollar amount per participant per plan year) and an aggregate (a total amount of plan claims per plan year). *Id.* Stop loss coverage is designed to protect the employer—and the plan—from catastrophic claims in any given plan year. *Id.*

256. In general terms, ERISA preempts any state law as it "relates to" an employee benefit plan. Employee Retirement Income Security Act of 1974, § 514(a), 29 U.S.C. § 1144(a)

the plan because of the reinsurer's act of selling coverage to the plan and paying claims under the reinsurance policy.[257]

D. *Renewal and a Participant's Refusal to Authorize Release of PHI*

What if the employer is faced with a renewal situation that requires the employer to obtain additional PHI from a plan participant? For example, during the underwriting process, the insurance company requests that the participant's health care provider submit detailed medical information for review, in addition to the claim history provided from the plan (now PHI under the Act). The claims information could be provided to the insurance company, provided such practice is contemplated by the plan's HIPAA amendment. As for the medical records request, there is a clear need for a HIPAA authorization from the participant to

---

(2000). According to the United States Supreme Court, "[a] law 'relates to' an employee benefit plan, in the normal sense of the phrase, if it has a connection with or reference to such a plan." Shaw v. Delta Air Lines, Inc., 463 U.S. 85, 96-97 (1983) (citing BLACK'S LAW DICTIONARY 1158 (5th ed. 1979)). *But see* N.Y. State Conference of Blue Cross & Blue Shield Plans v. Travelers Ins. Co., 514 U.S. 645, 655-56 (1995) ("We simply must go beyond the unhelpful text and the frustrating difficulty of defining [§ 1144(a)'s] key term ["relating to"], and look instead to the objectives of the ERISA statute as a guide to the scope of the state law that Congress understood would survive."). However, ERISA contains a savings clause under which state insurance laws are exempted from the application of the ERISA preemption provision, provided the state law regulates the business of insurance. 29 U.S.C. § 1144(b)(2)(A) (2000). The United States Supreme Court has held that self-funded plans are not in the business of insurance, and are not subject to state laws. *See* FMC Corp. v. Holliday, 498 U.S. 52, 61 (1990). The Supreme Court, in its current term (2002-2003), has redefined the ERISA preemption analysis of state insurance laws. *See* Ky. Ass'n of Health Plans, Inc. v. Miller, No. 00-1471, 2003 WL 1726508, at *1 (U.S. Apr. 2, 2003) (articulating a new two part test, which requires an analysis of whether (1) the state law is "specifically directed toward entities engaged in insurance"; and (2) the state law "substantially affect[s] the risk pooling arrangement between the insurer and the insured," and abandoning use of the McCarran-Ferguson Act and related case law in the preemption analysis). As to the issue of stop loss coverage, the courts have consistently held that stop loss coverage does not automatically convert the plan into an insured plan, provided the coverage is not directly insuring the plan participants. *See, e.g.*, Bill Gray Enters. v. Gourley, 248 F.3d 206, 215 (3d Cir. 2001) (cautioning in dicta that purchasing a large amount of stop loss coverage may indicate that the plan is attempting to retain the financial security of insurance and reap the benefits of ERISA preemption); Am. Med. Sec., Inc. v. Barlett, 111 F.3d 358, 364 (4th Cir. 1997) (holding that Maryland insurance regulations crossed the line of preemption when they deemed self-funded plans to be insured plans when the attachment point of the stop-loss insurance was too low); Lincoln Mut. Cas. Co. v. Lectron Prod., Inc., 970 F.2d 206, 210 (6th Cir. 1992) (holding that ERISA preempted application of Michigan law even though the self-funded plan had stop loss insurance for losses in excess of $75,000). The Department of Labor has opined that stop loss insurance is not a plan asset if contracted by, and the proceeds are paid to, the employer. Pension Welfare Benefits Administration, Advisory Opinion Letter, 92-02A (Jan. 17, 1992).

257. *See* Dec. 3, 2002 Guidance, *supra* note 1, at 53 ("However, a business associate relationship could arise if the reinsurer is performing a function on behalf of, or providing services to, the health plan that do not directly relate to the provision of the reinsurance benefits.").

direct the health care provider to release the necessary information to the employer and the underwriter. What happens if the participant refuses? The Privacy Rule clearly states:

> A covered entity *may not* condition the provision to an individual of treatment, payment, enrollment in the health plan, or eligibility for benefits on the provision of an authorization, except:
>
> . . . .
>
> (ii) A health plan may condition enrollment in the health plan or eligibility for benefits on provision of an authorization requested by the health plan *prior to* an individual's enrollment in the health plan, if:
>
> (A) The authorization sought is for the health plan's eligibility or enrollment determinations relating to the individual or for its underwriting or risk rating determination; and
>
> (B) The authorization is not for a use or disclosure of psychotherapy notes under paragraph (a)(2) of this section.[258]

Thus, a participant cannot be refused participation in the plan, assuming that such refusal would be interpreted to be adverse action against an individual who is unwilling to disclose his or her PHI.[259] However, the insurer may simply refuse to underwrite the group because of a failure to obtain the necessary information, or alternatively, the insurer may agree to underwrite the group only if that individual is not covered by the insurer. It is difficult to imagine that either result was contemplated when the Privacy Rule was written.[260]

In reading the Privacy Rule, obtaining the participant's authorization[261] prior to the time of enrollment is key in determining the latitude a plan has in denying a participant eligibility or benefits under the plan upon a refusal to provide the authorization.[262] Such an authorization would need to be prepared to meet the core elements required by the Privacy Rule.[263] The authorization would also need to be narrowly drafted to follow the permissible reasons that the plan can seek an authorization prior to enrollment, including: to determine an individual's eligibility for coverage, to determine enrollment under the plan, and for underwriting and risk determination.[264] A statement of the consequences for

---

258. 45 C.F.R. § 164.508(b)(4)(ii)(A)-(B) (emphasis added).

259. *See id.*

260. No comments appear in the preamble to the revised Privacy Rule that discuss this dilemma. The issue was addressed in the preamble to the original Privacy Rule.

261. A separate authorization would be needed for each plan participant, which in an employer group plan would include the employee, and if applicable, the employee's spouse and dependent children (using the personal representative requirements under the Privacy Rule).

262. *Id.* § 165.508(a)(4)(ii).

263. *See* discussion *supra* Part II.B.3.

264. *See* 45 C.F.R. § 164.508(b)(4)(ii)(A)-(B).

refusing to sign the authorization must be clearly set forth in the authorization.[265] Employer plan sponsors would not be permitted access to psychotherapy notes under this preenrollment authorization form, but could obtain a separate authorization for the use and disclosure of the notes.[266] If the individual was unwilling to provide this information, no adverse action could be taken against the individual.[267] Due to the fact that the authorization would also need to remain in effect during the period of participation in the plan, the authorization would need to use "an expiration event" rather than an expiration date for termination of the authorization. The plan document may already contain a standard provision regarding denial of benefits or enrollment if a participant does not authorize the release of the health information. This provision would need to be included in a "HIPAA version" of the plan, both as part of the HIPAA plan amendment and the plan's privacy notice. The plan enrollment form—which, because of the Act's authorization requirements, should be a separate document from the authorization[268]—should also cross-reference the Act's authorization requirement for participation and continued benefits under the plan, as well as the consequences for failure to provide authorization.

If a plan fails to obtain the necessary authorization prior to enrollment, it appears that the plan could not deny a participant benefits based on a refusal to release PHI to the underwriter.[269] But what if the employer, in the process of

---

265. 45 C.F.R. § 164.508(c)(2)(ii)(B).

266. *See* Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. 53,182-53,223 (Aug. 14, 2002) (to be codified at 45 C.F.R. pt. 160).

267. The preamble to the revised Privacy Rule contains a direct response to this issue:

> The Privacy Rule does not permit a health plan to condition enrollment, eligibility for benefits, or payment of a claim on obtaining the individual's authorization to use or disclose psychotherapy notes. Nor may a health care provider condition treatment on an authorization for the use or disclosure of psychotherapy notes. In a situation such as the one described by the commenter, the Department would look closely at whether the health plan was attempting to accomplish indirectly that which the Rule prohibits. These prohibitions are to ensure that the individual's permission is wholly voluntary and informed with regard to such an authorization. To meet these standards, in the circumstances set forth in the comment, the Department would expect the provider subject to such a requirement by the health plan to explain to the individual in very clear terms that, while the provider is required to ask, the individual remains free to refuse to authorize the disclosure and that such refusal will have no effect on either the provision of treatment or the individual's coverage under, and payment of claims by, the health plan.

Id. The accompanying comment reads: "One commenter asked for clarification that a health plan may not condition a provider's participation in the health plan on seeking authorization for the disclosure of psychotherapy notes, arguing that this practice would coerce providers to request, and patients to provide, an authorization to disclose psychotherapy notes." *Id.*

268. *See* discussion *supra* Part III.B.3.

269. *See* 45 C.F.R. § 164.508(b)(4)(ii)(A)-(B).

obtaining stop loss coverage to cap and insure its self-funding risk, requests an authorization from an employee plan participant? Would the preenrollment exception still apply? Read carefully, the exception is only applicable to the health plan and the plan's underwriting process, *not* the employer in its underwriting process.[270] Because the authorization requirement and prohibition against adverse action rests with the covered entity, it appears that the employer as a noncovered entity could take such adverse action and deny participation in the plan.

E. *The Role of the Third-Party Administrator*

For most employers that sponsor a self-funded health plan, administration of the plan is performed by a third-party administrator (TPA) under a written agreement between the employer and the TPA. Typically, the TPA is responsible for the preparation of plan documents, obtaining the network of providers to deliver health care services to the plan participants, providing case management and utilization review services, and claims processing and payment, among other things. Under the Act, the TPA is not treated as a covered entity,[271] but in its capacity as a business associate of the plan, it would be required to comply with the Privacy Rule.[272]

It is clear that the Privacy Rule contemplates that the relationship of the TPA is with the plan itself, rather than the employer. The December 2002 OCR Guidance lists claims processing and administration, data analysis, utilization review, and benefit management as business associate activities.[273] Going forward, TPA agreements will need to be drafted to reflect that the agreement

---

270. *See id.*

271. If the TPA processes claims, it may be considered a health care clearinghouse and thus a covered entity under the Act. *See id.* § 160.103 (defining health care clearinghouse); *see also* discussion *supra* Part III.A.2. A health care clearinghouse has distinct compliance obligations under the Act if it is acting as the business associate of another covered entity. *See* 45 C.F.R. § 164.500(b)(1).

272. Dec. 3, 2002 Guidance, *supra* note 1, at 110. The Guidance goes on to note:

> [P]roviding services to or acting on behalf of a health plan does not transform a third party administrator (TPA) into a covered entity. Generally, a TPA of a group health plan would be acting as a business associate of the group health plan. Of course, the TPA may meet the definition of a covered entity based on its other activities (such as providing group health insurance).

Id. (citing 45 C.F.R. § 160.103).

273. *See id.* at 34-35 (listing among examples of business associates a "third party administrator that assist[s] a health plan with claims processing").

between the plan (not the employer)[274] and the TPA will include the standards contained in the Privacy Rule for disclosures to business associates.[275]

Many employers may look to their TPAs to perform the plan's HIPAA compliance functions. While the Privacy Rule permits these responsibilities to be performed by a third party under agreement, the compliance obligation under the Privacy Rule remains with the employer.[276] TPAs may decide to offer the Act's compliance services much like Consolidated Omnibus Budget Reconciliation Act compliance as an additional service under the TPA agreement for an additional per covered life cost.

Indemnification from the TPA to the plan for TPA errors in the Act's administration will likely be demanded by the plan. While there is no private right of action under the Act (eliminating plan participant claims), the fact that the Privacy Rule requires a HIPAA plan amendment has the effect of creating a private right of action for such failures using ERISA remedies. Participants may bring breach of fiduciary duty claims against the plan and the employer as the plan sponsor and plan administrator.[277] While many errors and omissions policies may exclude the Act's violations per se, if the claim is made in the context of plan administration (albeit HIPAA related) coverage for errors may exist. All of these issues should be taken into consideration when drafting an indemnification clause.

F. *Marketing to Group Health Plan Participants*

Some of the most restrictive provisions on the disclosure of PHI exist in the Act's marketing rules.[278] Insurance professionals must evaluate their marketing efforts and their use of plan participants' PHI that has been obtained through their relationship with the group health plan, and the employer as plan sponsor to ensure these efforts fall within the Privacy Rule's requirements. Plan sponsors should understand these efforts. If a business associate agreement is in place between the parties, the insurance professional should be engaging in activities on behalf of the covered entity and not itself (that is, not marketing the insurance entity's products and services to plan participants).[279] Additionally, the

---

274. The employer, as the plan sponsor, will be the signatory and the party binding the plan to the agreement.

275. 45 C.F.R. § 164.502(e)(1). The Privacy Rule mandates a written document. *Id.* § 164.502(e)(2); *see also* discussion *supra* Part III.A.5 (discussing business associates).

276. *See* discussion *supra* Part IV.A.

277. *See* Varity Corp. v. Howe, 516 U.S. 489 (1996) (permitting plan participants' individual claims for fiduciary breach against the plan fiduciaries).

278. Perhaps better described as the marketing prohibitions.

279. Dec. 3, 2002 Guidance, *supra* note 1, at 62-63. The Privacy Rule contains limited exceptions to this prohibition relating to plan enhancements and related products.

insurance professional should be contractually bound to the Act's marketing rules.[280] The Privacy Rule defines the term marketing,[281] and, except for treatment, payment, health care operations, and certain other limited exceptions, the Privacy Rule requires individual authorization for all uses and disclosures of PHI.[282]

In the OCR Guidance document, the section devoted to marketing contains a number of frequently asked questions regarding health plans and insurance professionals and their marketing efforts under the Act.[283] For example, a communication from a health insurer promoting home and casualty insurance products from the same company would require an authorization,[284] but if such communication were face-to-face, it would be acceptable under the Privacy Rule, without an authorization.[285] While the cross-selling of nonhealth-related insurance products to plan participants may be rare in practice, there are likely to be situations where an insurance entity may wish to promote health insurance conversion policies, disability policies, or Medicare gap policies to plan participants. In addition, there may be instances when the insurance entity wishes to promote wellness programs or enhanced benefits under the group health plan. Whether an authorization is required in these situations centers on the Act's definition of marketing activities versus treatment or health care operation activities.

---

280. *Id.* Sale of PHI to third parties for marketing purposes is also prohibited unless authorized by the participant. *Id.* Because the group health plan has the ultimate responsibility for a business associate's noncompliance with the Act, it will be interesting to see the extent to which plan sponsors attempt to protect the use of PHI by the insurance entities for marketing purposes. In many cases, the insurance professional may have easier access to identifiable information through claims processing and other services provided to the group health plan. While the unauthorized use of participant PHI should be less of an issue with fully insured plans due to the fact that the health insurer is a covered entity and subject to the Act directly, the situation that poses the greater risk of impermissible disclosure is the self-funded plan context, and the use of this information by the plan's TPA.

281. 45 C.F.R. § 164.501 (2002).

282. *Id.* § 164.508(a)(3)(i)-(iii).

283. Dec. 3, 2002 Guidance, *supra* note 1, at 69-76.

284. *Id.* at 69.

285. *See id.* at 75. The Guidance provides:

> Q: Must insurance agents that are business associates of a health plan seek a prior authorization before talking to a customer in a face-to-face encounter about the insurance company's other lines of business?
>
> A: No. In the specific case of face-to-face encounters, the HIPAA Privacy Rule allows health plans and their business associates to market both health and non-health insurance products to individuals.

Id. In practice, falling under the face-to-face exception would likely occur as a result of the insurer coming to the employer's campus to promote the insurance company's other products. *See id.*

The Privacy Rule marketing definition is broad and encompasses any "communication about a product or service that encourages recipients of the communication to purchase or use the product or service," or an arrangement between a covered entity and a third party, by which a disclosure of PHI is for direct or indirect remuneration, and will be used for communication to encourage use or purchase of a product or service.[286] A communication is not a marketing activity (and thus not subject to plan participant authorization) if it is made:

> (i) To describe a health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of, the covered entity making the communication, including communications about: the entities participating in a health care provider network or health plan network; replacement of, or enhancements to, a health plan; and health related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits; (ii) For treatment of the individual; or (iii) For case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual.[287]

In practice, this would seem to limit the ability of the insurance entity to discuss any product or service that did not have a direct nexus to the group health plan. Examples of communications that are not considered marketing include communications regarding disease management, health promotion, preventative care, or wellness programs of the covered entity or operated by the business associate on behalf of the covered entity, general health or wellness promotional materials, descriptions of the benefits contained in the health plan, descriptions of health care providers within a network serving the plan, notices about changes, improvements and replacement to the existing plan, and value-added items or services.[288] Current practices will need to be reviewed by the insurance professional and confirmed by the employer-plan sponsor to determine whether they fall within these exceptions. Otherwise, authorizations that are specifically tailored to the use of participant PHI for marketing purposes would need to be included as part of the enrollment process. Employers may be reluctant to require their employees to sign such authorizations for a variety of reasons, including the fact that benefit enrollment periods can be the busiest time of the year for human resources professionals, and may impose additional work without any obvious benefit.

The group health plan as a HIPAA covered entity poses many issues for employers and the insurance professionals that provide services to the plan and

---

286. 45 C.F.R. § 164.501.
287. *Id.*
288. Dec. 3, 2002 Guidance, *supra* note 1, at 64.

employer. The key in understanding the compliance obligations of both entities is a careful and thoughtful analysis of their relationships with the group plan and each other. With the delayed implementation date for small employer plans, the OCR has the opportunity to provide additional guidance on administration of these plans in a HIPAA environment.

V. A CASE HISTORY: A PATIENT'S PROGRESS THROUGH A COURSE OF TREATMENT—HOW USES AND DISCLOSURES OF INFORMATION WILL BE AFFECTED UNDER HIPAA

The following scenario illustrates how the Act will affect the delivery of health care, the effect it will have on the privacy protections afforded medical information, and a patient's confidence that his or her medical information is adequately protected.

Mrs. Public arrives at her local physician's office on April 14, 2003 for her scheduled appointment. She has read about this new Privacy Rule and is curious about what changes she will see as a result of its implementation. As she approaches the receptionist area, she notices a yellow line several feet back from the counter and a sign that requests she remain behind the line until the receptionist is finished with the patient ahead of her. This is Mrs. Public's first encounter with the impact of the Privacy Rule. Mrs. Public asks about this new sign and is told this is their effort to take reasonable safeguards to protect an individual's health information by limiting incidental disclosures.[289]

As she is being checked in, the receptionist hands Mrs. Public a Privacy Notice.[290] Mrs. Public also notices that there is a display case with extra copies of the notice on the counter.[291] The notice is in nine-point type and is eight pages long. The receptionist explains to Mrs. Public that this notice is a new federal requirement, and that the brochure contains information about how the physician's office uses and discloses protected health information and informs the patient about her rights and how to exercise those rights. She continues by explaining that the notice explains the physician's office responsibilities with respect to protecting Mrs. Public's health information, and who to contact if she wants further information. Mrs. Public is decidedly overwhelmed, but agrees to sign the form the receptionist hands her, acknowledging she has received a copy of the notice.[292]

---

289. *See* 45 C.F.R. § 164.530(c); Dec. 3, 2002 Guidance, *supra* note 1, at 15.
290. *See* 45 C.F.R. § 164.520(c)(2)(i)(A).
291. *See id.* § 164.520(c)(2)(ii)(B).
292. *See id.* § 164.520(e).

copy of her records. She receives a copy of her records within thirty days of her request and is billed for the copying costs plus postage.[301]

In reviewing her medical records, Mrs. Public notes that the past medical history in the admit note references her past history of obesity. Mrs. Public is distressed with this reference. She writes to the hospital, per the instructions in the Privacy Notice, and requests to have this information redacted from the medical record.[302] The hospital responds within sixty days to Mrs. Public's request, and denies the request, stating that the attending physician believes this information to be correct.[303] In addition, the denial letter explains to Mrs. Public that she has the right to submit a written statement disagreeing with the denial, and that this will become a permanent part of the medical record and will be included in any future disclosures of protected health information that is the subject of the amendment.[304] Mrs. Public prepares her disagreement letter and forwards it to the hospital for inclusion in the medical record.[305]

In follow up to this denial of the amendment, Mrs. Public decides it is very important for her to know who may have accessed her medical records, and contacts the Health Information Management Office again to request an accounting of disclosures of her protected health information. In response, the hospital notifies her within sixty days that her records were disclosed to the State Health Registry, as part of their required reporting of cancer cases. In addition, she is provided the name and contact information of a cancer researcher who accessed her information through an approved Privacy Board waiver of authorization.[306] Once again Mrs. Public is surprised at how her protected information can be shared with individuals without her prior knowledge or express authorization.

Several weeks after discharge, Mrs. Public receives a solicitation in the mail from the hospital's Foundation Office, providing her with information on how she might make a donation to support the hospital.[307] Mrs. Public is still upset over her interaction involving the denial of the amendment request, and is not interested in receiving such information in the future. She notes that the solicitation contains an address for her to write to remove her name from any

---

301. *See id.* § 164.524(c)(4) (providing that a covered entity may charge a reasonable fee for copying and postage). Previously, hospitals would include an additional processing fee in their fees.

302. *See id.* § 164.526(a).

303. *See id.* § 164.526(d)(1).

304. *See id.*

305. *See id.*

306. *See id.* § 164.528.

307. *See id.* § 164.514(e)(3).

further contacts with the Foundation Office. Mrs. Public writes the foundation and requests to be removed from their list.[308]

In the months following her hospitalization, Mrs. Public continues to receive outpatient chemotherapy services at the hospital. During this time, she is contacted by the hospital's marketing department about a new antiemitic drug treatment and how she might obtain information about this new drug.[309]

Mrs. Public decides to try the new drug and sends her daughter to pick up her prescription. The daughter is handed the Pharmacy's Privacy Notice and asked to sign a log acknowledging receipt of the notice.[310]

One year later, Mrs. Public returns to the hospital for a follow-up check-up. She receives the bad news that her tumor has returned and she will require additional surgery. Wishing to minimize the impact on her family, Mrs. Public requests that information on her follow up appointment be sent to a post office box until such time as she decides to share information on her recurrence with her family. The hospital agrees to comply with this request and modifies its appointment reminder system to send the notice to an alternative address.[311] Mrs. Public is pleased that the hospital accommodates this request. However, as she starts the process again of routine access to health care, Mrs. Public is left wondering if the protection of her health information has at all been improved with the Privacy Rule.

VI. CONCLUSION

The Privacy Rule will pose a number of challenges to the entities it covers. Its provisions are complex and are subject to a number of interpretations. In addition, it is not clear how the preemption principles will work to supplant state law, and further, it is problematic how courts will interpret those principles. Further, the challenges to group health plans and the insurance professionals that provide services to the plan and the employer are significant. Most importantly, while it is clear that the Privacy Rule will be difficult and costly to implement, it is not clear whether the administrative burdens it poses will result in any greater protection of the health information it seeks to protect.

---

308. *See id.* § 164.514(f)(1)(iii) (requiring that covered entities allow individuals to opt out of receiving fundraising requests).

309. *See id.* § 164.501 (providing that information on alternative treatments is not considered marketing, and therefore allowed under the Privacy Rules without patient authorization).

310. *See* Dec. 3, 2002 Guidance, *supra* note 1, at 14 (noting health care professionals may discuss a patient's condition with family members).

311. *See* 45 C.F.R. § 164.522(b)(1)(i).


DRAKE UNIVERSITY
VERITAS
1881