Journal of Health Law

Spring 2004 Volume 37, No. 2

Application of the HIPAA Privacy Rule to Employer Benefit Plans and A Compliance Theory of Statutory Interpretation

Barbara Bennet

AMERICAN HEALTH LAWYERS

SAINT LOUIS UNIVERSITY SCHOOL OF LAW

Application of the HIPAA Privacy Rule to Employer Benefit Plans and A Compliance Theory of Statutory Interpretation

*Barbara Bennett**

ABSTRACT: The application of the federal privacy regulations promulgated pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) to employer benefit plans is arguably the most conceptually difficult area of a complex law. A purely textual reading of the Rule, when applied to employer plans, results in varying interpretations on some significant issues and puzzling results on others. This Article offers a practical approach for interpreting the rule when clear-cut answers are not provided by the text and DHHS guidance is nonexistent or unclear. In addition, this approach can be applied to the interpretation of other statutes and regulations.

The application of the federal privacy regulations (Privacy Rule or Rule)[1] promulgated pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA)[2] to employer benefit plans is arguably the most conceptually difficult area of a complex law. A purely textual reading of the Rule, when applied to employer plans, results in varying interpretations on some significant issues and puzzling results on others. The Department of Health and Human Services (DHHS), which issued the Rule, and the Office for Civil Rights (OCR), which is responsible for its enforcement,[3] failed to clarify most of these issues[4] in the preamble and various other guidance accompanying the final Rule.[5]

This Article offers a practical approach for interpreting the Rule when clear-cut answers are not provided by the text and DHHS

* Ms. Bennett is a partner at Hogan & Hartson LLP in Washington, D.C.

guidance is nonexistent or unclear. In addition, this approach can be applied to the interpretation of other statutes and regulations. The Article also addresses the relationship between the proposed approach to the ongoing lively debate and dynamic development of the jurisprudence of statutory interpretation. Further, it discusses the usefulness of the approach for businesses and their lawyers struggling with current corporate governance compliance issues.

Commentators already have begun to proffer paradigms for judging HIPAA's effectiveness that may offer courts some philosophical bases for resolving HIPAA interpretation conundrums. In point-counterpoint articles published in the *Minnesota Law Review* June 2002 symposium issue on *Modern Studies in Privacy Law*,[6] Professors Lawrence Gostin and James Hodge suggest a balancing test between individual and communal interests as the proper backdrop for the Rule.[7] Meanwhile, Professor Peter Jacobson proposes a modified rule of reason approach with a presumption for privacy.[8] While each approach has its philosophically appealing attributes, both articles offer their tests as ones against which the Rule itself should be evaluated rather than as specific guidance for resolving ambiguities in that Rule. These approaches are tailored specifically to evaluate HIPAA, rather than for use generally to evaluate statutes or regulations. Moreover, the tests offer policy-based balancing more appropriate for judicial application or theoretical academic analyses, as opposed to the type of specific direction that is helpful to companies implementing compliance.

Unlike the symposium articles, the framework offered in this Article provides direction for interpreting statutes and regulations for purposes of required compliance when varying interpretations appear possible. The framework proposes the analysis of each possible interpretation under four factors: (1) the extent to which the interpretation is consistent with the text of the law (Textual Test); (2) the extent to which the interpretation is consistent with the legislative history or official agency guidance (Commentary Test); (3) the extent to which the interpretation furthers the stated purposes of the law (Purposes Analysis); and (4) the extent to which, when applied to actual facts, the interpretation avoids producing an absurd result (Absurdity Analysis). The last prong of the approach, avoiding an absurd result, is used in this Article as a shorthand reference to the entire analytical framework (Absurdity Avoidance).

The Absurdity Avoidance framework, when applied to the HIPAA Privacy Rule, provides the philosophical underpinnings for judging the effectiveness of the Rule. Reality has an ability to "zero in"

on the absurd that is often missed by academics and government bureaucrats dealing with issues in the abstract.

Part I of this Article sets forth the general Privacy Rule requirements for employer-sponsored health plans. Part II analyzes the impact of those requirements on the most common forms of employer plans. Part III describes the Absurdity Analysis, including how the analysis relates to other theories of statutory interpretation and to current corporate governance developments. Part IV identifies and analyzes two areas of application and interpretation issues with respect to the impact of the Privacy Rule on employer health plans. These issues merit further discussion because they were left unclear or were unanticipated by the provisions of the Rule. Specifically, the areas addressed are: the application of the Rule to healthcare flexible spending accounts, employee assistance programs, and to "other health plans" in the employer context; and the limits on the use of enrollee authorization by employers to avoid certain Privacy Rule compliance requirements. Within these areas, the specific issues addressed include: (1) whether, and to what extent, employee assistance programs (EAPs) are subject to the Rule; (2) whether, in the employer context, the Rule applies only to employee welfare benefit plans regulated under the Employee Retirement Income and Security Act of 1974 (ERISA);[9] (3) how certain plans, such as healthcare flexible spending accounts and EAPs, that are ERISA plans, but do not meet the definition of "insured" or "self-insured" are regulated under the Rule; (4) whether employers may utilize authorizations to avoid the Rule's compliance requirements dealing with receipt of protected health information for final appeals determinations; and (5) whether employers may circumvent the Rule's prohibition on the use of protected health information from a covered health plan for purposes of administering other benefit plans.[10] Finally, Part V evaluates reasonable interpretations for each issue addressed in Part IV under the Absurdity Avoidance framework, resulting in guidance for resolution of these issues and providing an example of the analysis that may be applied generally to other laws.

I. Privacy Rule Background

A. Definition of Health Plans Under the Privacy Rule

While employers are not Covered Entities under the Privacy Rule,[11] certain health plans sponsored by employers are Covered Entities and, in many cases, are subject to the full spectrum of Privacy Rule compliance requirements.[12] A health plan that is a Covered Entity under HIPAA (Health Plan)[13] is an individual or group plan that provides, or pays the cost of, medical care.

The Rule cites Section 2791(a)(2) of the Public Health Service Act (PHS Act) for the definition of "medical care" and specifically includes items and services paid for as medical care.[14] The PHS Act defines medical care as: (A) amounts paid for diagnosis, cure, mitigation, treatment, or prevention of disease, or amounts paid for the purpose of effecting any structure or function of the body; (B) amounts paid for transportation that is primarily for and essential to medical care referred to in (A); and (C) amounts paid for insurance covering medical care referred to in (A) and (B) (Medical Care).[15]

This definition of a Health Plan specifically includes employee welfare benefit plans as defined in ERISA[16] to the extent they provide or pay for Medical Care (Group Health Plans)[17] and "[a]ny other individual or group plan . . . that provides or pays the cost of" Medical Care (Catchall Category).[18]

Health Plans specifically exclude plans or programs that provide or pay for excepted benefits listed in Section 2791(c)(1) of the PHS Act (Excepted Benefits).[19] These Excepted Benefits include accident or disability income insurance, liability insurance, worker's compensation, and coverage for on-site medical clinics.[20] An exception exists, however, under the Privacy Rule for Group Health Plans that are administered by a third party and have fewer than fifty participants.[21] In addition, plans with annual receipts of $5 million or less are considered "small health plans"[22] and were not required to comply with the Privacy Rule until April 14, 2004.[23] All other Health Plans were required to comply by April 14, 2003.[24]

Group Health Plans usually do not have a separate corporate presence and are dependent on the plan sponsor or another third party for administration and operations support. In addition, due to its dual nature as both employer and plan administrator, an employer often provides plan administration functions and, thus, has a legitimate need for information, including protected health information,[25] from its Group Health Plans. The relationship between an employer and the Group Health Plans it sponsors creates two main categories of issues for the employer under the Privacy Rule. With respect to any Group Health Plan, the categories are:

(i) Ensuring compliance with the Privacy Rule by the Group Health Plan itself; and

(ii) Ensuring compliance with the Privacy Rule by the employer in its role as sponsor with respect to its receipt of protected health information from the Group Health Plan.

B. Privacy Rule Requirements for Health Plans

Compliance by Health Plans with the Privacy Rule can be quite burdensome and compels such Covered Entities to comply with a long list of requirements. Thus, Health Plans must: (i) use and disclose protected health information only as permitted under the Rule, limited by the "minimum necessary" requirements,[26] and subject to the numerous exceptions and qualifications applicable to Covered Entities;[27] (ii) obtain special authorization for any other uses and disclosures not permitted under the Rule;[28] (iii) provide a written notice of privacy practices to plan beneficiaries;[29] (iv) enter into Business Associate Agreements with entities that create or receive protected health information in the course of providing certain services to or on behalf of the plan;[30] (v) appoint a privacy officer and establish a contact for privacy-related complaints by plan beneficiaries and a complaint mechanism;[31] (vi) create and implement policies and procedures allowing beneficiaries to access and copy their protected health information, request restrictions on or confidential communications of their protected health information, request amendments to the information, and request an accounting of certain types of disclosures (Individual Rights);[32] (vii) develop and implement policies and procedures to ensure compliance with the Rule, including the minimum necessary requirements; (viii) provide appropriate training to all members of the plan's workforce; (ix) implement appropriate administrative, physical, and technical safeguards to protect the privacy of protected health information; (x) adopt and apply appropriate sanctions against workforce members for violations of the Rule or the plan's policies and procedures; (xi) mitigate any known, harmful effects caused by any violation of the Rule or the plan's policies and procedures; (xii) refrain from taking intimidating or retaliatory actions against individuals who exercise their rights under the Rule; (xiii) refrain from requiring individuals to waive their rights under the Rule as a condition of treatment, payment, enrollment, or eligibility; and (xiv) document adherence to these requirements as provided in the Rule.[33] These obligations are referenced in this Article collectively as "Health Plan Requirements."

Health maintenance organizations (HMOs) and other insurance issuers are Health Plans and must themselves comply with the Privacy Rule. As such, if a Group Health Plan contracts with an HMO or insurance issuer to fully insure its benefits and does not create or receive protected health information (except for summary health information[34]) or enrollment or disenrollment information,[35] the Group Health Plan can avoid most of these burdensome Health Plan Requirements.[36]

On the other hand, to the extent that the Group Health Plan is self-insured or creates or receives protected health information (other than summary health information or enrollment and disenrollment information), it retains ultimate compliance responsibility and must meet all the Health Plan Requirements. A Group Health Plan can try to negotiate with third-party administrators to transfer contractually all or part of the administrative burden of compliance.[37]

C. Privacy Rule Requirements for Health Plan Sponsors

The Privacy Rule does not apply directly to employers, but it indirectly requires compliance by employers in certain instances.[38] Thus, in addition to ensuring that Group Health Plans comply with the Health Plan Requirements, an employer in many instances must comply with the Privacy Rule in its role as plan sponsor and employer. It will be prudent for employers to focus on this compliance because of the potential criminal penalties under HIPAA associated with knowingly receiving improperly disclosed protected health information.[39]

Absent an authorization from the affected individual, the Privacy Rule allows for the disclosure of protected health information by a Group Health Plan, including HMOs or insurance issuers with respect to the Group Health Plan,[40] to the plan sponsor for the purpose of carrying out plan administration functions.[41] This disclosure is allowed provided that the sponsor amends the plan documents to include: (i) a description of the permitted uses and disclosures of enrollee protected health information by sponsor employees providing plan administration functions;[42] (ii) adequate separation between the Health Plan and employer;[43] and (iii) a provision that the Health Plan shall disclose enrollee protected health information to the employer only upon receipt of a certification that the plan documents have been amended to incorporate the provisions described in the following paragraph and that the employer, in its capacity as plan sponsor, shall comply with the numerous sponsor requirements mandated by the Rule.[44]

Specifically, the sponsor shall: (i) not use or further disclose enrollee protected health information other than as permitted or required by the plan document or as required by law; (ii) ensure that any contractors, including a subcontractor, to whom the employer or workforce members provide enrollee protected health information received from the Health Plan, agree to the same restrictions; (iii) not use or disclose enrollee protected health information for employment-related actions and decisions unless authorized by

an individual enrollee; (iv) not use or disclose enrollee protected health information in connection with any other benefit or employee benefit plan of the employer unless authorized by an individual enrollee; (v) report to the Health Plan privacy officer any enrollee protected health information use or disclosure that is inconsistent with the uses or disclosures provided for; (vi) make enrollee protected health information available to an individual in accordance with 45 C.F.R. § 164.524; (vii) make enrollee protected health information available for amendment and incorporate any amendments to enrollee protected health information in accordance with 45 C.F.R. § 164.526; (viii) make available the information required to provide an accounting of disclosures in accordance with 45 C.F.R. § 164.528; (ix) make internal practices, books, and records relating to the use and disclosure of enrollee protected health information received from the Health Plan available to the Secretary of DHHS for the purposes of determining the Health Plan's compliance with the Privacy Rule; and (x) where possible, return or destroy all enrollee protected health information received from the Health Plan that the employer or workforce members still maintain in any form, and retain no copies of such enrollee protected health information when no longer needed for the purpose for which disclosure was made.[45] These obligations to amend plan documents and to certify compliance with requirements (i) through (x) are the "Sponsor Requirements."

It is important to note that the Privacy Rule allows a Group Health Plan to share certain limited protected health information with the plan sponsor in two situations without the plan or the sponsor having to meet these Sponsor Requirements. Specifically, a Group Health Plan may, without individual authorization, amend the plan documents or by provision of the Certification by the plan sponsor share with the sponsor: (i) summary health information for the limited purposes of obtaining premium bids for health insurance coverage or modifying, amending, or terminating the Group Health Plan; and (ii) enrollment and disenrollment information.[46]

II. Impact of Privacy Rule on Employer Group Health Plans

Employers typically sponsor one or more of the following employee benefit plans: medical, including prescription and behavioral health benefits; dental; vision; smoking cessation and other wellness plans; an EAP; an executive health program; travel/accident plan; life insurance; short- and long-term disability; healthcare and dependent-care flexible spending accounts (FSAs); and worker's compensation.

The disability programs, life insurance programs, dependent care FSA, and worker's compensation insurance coverage are not Health Plans and, thus, are not subject to the Privacy Rule.[47] Disclosure by Health Plans or covered providers of PHI to these other programs or their sponsors, however, is subject to the Privacy Rule and may be done only in compliance with the Rule.[48]

The remaining plans typically sponsored by employers are medical, dental, vision, healthcare FSA, EAP, and other wellness programs. Benefits under medical, dental, and vision plans are either fully insured or self-insured by the employer.[49] The applicability of the Privacy Rule to these benefit plans and programs is analyzed in this section. The application of the Rule to FSAs, EAPs, and other wellness programs, which commonly are not provided under the same types of "fully-insured" or "self-insured" mechanisms, offer one of the three interpretation issues analyzed in Part III.

A. Insured Plans

Group Health Plans with insured benefits are subject to the Privacy Rule.[50] Although, if these benefits are provided by an insurance issuer or HMO and if:

(i) The plans (or the sponsor on the plans' behalf) do not create or receive any protected health information other than summary health information or enrollment or disenrollment information; and

(ii) The sponsor does not receive from the insurance issuer or HMO any protected health information other than summary health information or enrollment or disenrollment information,[51]

then the statutory obligations under the Privacy Rule will be only for the plans to:

(i) Refrain from any retaliatory or intimidating acts if an individual seeks to exercise rights under the Privacy Rule with respect to these plans;[52] and

(ii) Refrain from requiring individuals to waive their rights under the Privacy Rule as a condition of treatment, payment, enrollment in these plans, or eligibility for benefits.[53]

If the sponsor of a plan for which the benefits are provided by an insurance issuer or HMO does receive additional protected health

information from the insurance issuer or HMO, then the sponsor will be required to amend the plan documents and comply with the Sponsor Requirements.

B. Self-Insured Plans

The Privacy Rule provides that Self-Insured Group Health Plans must comply with all the Health Plan Requirements. Further, if the sponsor receives additional protected health information with respect to these plans, the sponsor will be required to amend the plan documents and comply with the Sponsor Requirements. In most cases, sponsors of self-insured plans receive additional protected health information in connection with their duties as plan fiduciaries to hear final appeals related to denial of enrollee benefits. In addition, because employers bear the ultimate costs of claims under these plans, they often need more detailed claims data for purposes of utilization review and disease management.

Most employers contract with third-party administrators (TPAs)[54] to handle the administrative functions of managing self-insured plans, including claims processing and payment. The Privacy Rule requires that Health Plans enter into Business Associate Agreements with any such TPAs that will receive or create protected health information on behalf of the Health Plan. The Business Associate Agreement requires the TPA to safeguard the protected health information and limits the TPA's use and disclosure of that information.[55] This contracting process[56] has resulted in some plans and sponsors transferring some of the plan's compliance responsibilities to the TPA, such as direct administration of Individual Rights or issuance of a privacy notice. At the same time, some TPAs are using the Business Associate Agreement as a vehicle for adding burdensome provisions not required by the Rule.[57]

The Privacy Rule requires that Health Plans impose Business Associate obligations on a TPA. Practically, it is also possible for a plan, through its sponsor, to contractually transfer the administrative burden for virtually all of the Health Plan Requirements to a willing TPA. In addition, if the TPA agrees to assume the sponsor's fiduciary responsibility under ERISA and serve as final claims adjudicator, the sponsor can decide not to receive any additional protected health information from or with respect to the plan. Thus, the sponsor avoids all the Sponsor Requirements.[58]

No employer, however, can escape the burden of carefully analyzing its benefit plans and programs. This burden includes identifying Health Plans, determining its compliance responsibilities, and developing and implementing a compliance program. In developing

this compliance program, each employer and its counsel will be faced with the need to make interpretation decisions concerning the Rule's application to that employer's operations where the issues are not clearly defined under the Rule. The following section describes the Absurdity Avoidance approach as a framework for making those decisions.

III. Practical Jurisprudence and the Case for Avoiding Absurdity

The analysis proposed in this Article consists of four tests to apply serially when evaluating various statutory or regulatory interpretations for compliance purposes. The analysis provides a structured way for individuals and entities to make a compliance decision when faced with ambiguous, vague, or incomplete rules of law. Courts and enforcement authorities also may find the analysis useful in determining violations. If a person has documented a decision or drafted a compliance plan based on this analysis, and a court or other authority finds the application of the analysis to be rational and in apparent good faith, no liability should exist. This remains true if the court or enforcement authority disagrees with the actual result. This approach is consistent with the contemporary development of compliance and the enforcement standards that consider compliance plans, training, and review systems to be key factors in determining liability.[59]

The Absurdity Avoidance approach is more practical and less lofty than other principles of statutory interpretation recently debated and discussed in the literature. Those theories are meant for legislators and judges who have the luxury of authority and discretion when making their decisions. For businesses faced with current deadlines and little real guidance—yet very real penalties—a different, more pragmatic approach is needed and warranted.

A. The Absurdity Avoidance Approach

1. The Textual Test

Scholars have dueled about the significance of legislative history to statutory interpretation,[60] but no author has argued with the primary importance of the text. No interpretation of a statutory or regulatory provision will or should survive scrutiny if that interpretation is not consistent with the text of that law. Despite one's motivation in molding a particular result, if that result is born of an interpretation contrary to the clear meaning of the rule of law at issue, the result is doomed. When making decisions about interpretations of law for compliance, careful thought and attention

should be directed to the precise wording of that law. Under the Absurdity Avoidance approach, interpretations that are consistent with the text of the law survive the Textual Test and move on to be measured against the second prong—the Commentary Test.

It may seem obvious that an issue would not reach the Commentary Test if it did not pass the Textual Test. In other words, an interpretation should be unclear only when more than one interpretation will fit the text of the Rule, and technically this is true. Sometimes, however, the tendency in making compliance interpretations is to read the Rule in the context of other considerations or one's own judgment. It is helpful to isolate the text and evaluate its application in a vacuum in order to identify the reasons and process for making any decision.

2. The Commentary Test

In a lawsuit, a party may legitimately take a position that is consistent with the text of a regulation and its enabling statute, but is contrary to the legislative history or an interpretation published by the promulgating body. When determining compliance policy, making a decision that is contrary to published commentary that was clearly meant to apply to the facts at hand entails too much risk and is unrealistic. Thus, the Commentary Test measures the consistency of any interpretation that survives the Textual Test against the legislative history, guidance, or interpretations issued by the executive or legislative body that promulgated the statute or regulation. This guidance serves as an expression of the intent of those who adopted or promulgated the law.

Violation of many rules and regulations carries civil and criminal penalties. Criminal penalties require intent, which can be inferred from a position contrary to that taken by published interpretations of the promulgating agency. It makes sense, therefore, to require in the case of textual vagueness or ambiguity that any resolution be consistent with interpretations published by the promulgating body. Indeed, even in cases in which the Textual Test produces what appears to be one clear result, failing to review the commentary can be risky. Thus, this second prong is a necessary step in all instances. If commentary exists relevant to the issue and if only one interpretation passes this second test, however, the inquiry can end at this point. The third and fourth prongs—the Purposes Analysis and the Absurdity Analysis—are more subjective tests that involve interpretation and balancing. They are appropriate only for cases in which multiple interpretations of the same law meet both the Textual Test and the Commentary Test.

3. The Purposes Analysis

If, after application of the Textual Test and the Commentary Test, multiple possible interpretations of the text continue to exist, each interpretation should be examined to determine to what extent it furthers the stated purposes of the relevant statute or regulation. The Purposes Analysis is the second, less direct and more subjective step toward attempting to determine the drafter's intent. If the intent is not spelled out in the commentary, perhaps it can be gleaned from the stated purposes of the law as applied to the application being studied.

If one or more interpretations are substantially consistent with the furtherance of one or more of the primary purposes of the law, then these interpretations survive. Stated another way, any interpretation that does not serve those purposes or is contrary to the furtherance of one or more of those purposes is conditionally eliminated. The elimination is conditional because the Purposes Analysis and the Absurdity Analysis are by their nature subjective balancing tests and, in the end, must be considered in concert.

4. The Absurdity Analysis

If one or more interpretations meet the Purposes Analysis, the next and final prong requires that any result not be absurd. If more than one result is obtained and neither is absurd, the least absurd is chosen. If all results are absurd, then one must reconsider any result that failed to pass the Purposes Analysis. If one of the discarded interpretations leads to a significantly less absurd result than the interpretations that passed the Purposes Analysis, a more complex balancing of these two prongs is required and a leap of faith is necessary. Nonetheless, the process will narrow the instances in which this must occur and, thus, reduce the overall compliance risk.

One may ask why absurdity must enter the equation at all when the reliable and ubiquitous concept of reasonableness stands as ready soldier to the task. The answer lies in the reasonable nature of reasonableness itself. When one thoughtfully considers the issue, the absurd is simply the obviously, unmistakably unreasonable. It is so unreasonable that it is more likely than not to prompt the reaction, "that's absurd!" The measuring of one statutory interpretation against another, based on which is the more reasonable, carries with it the assumption that each is a reasonable result. If more than one interpretation is reasonable, it makes more sense to revert to the Purposes Analysis and evaluate the intent of the drafters rather than to substitute one's own values to determine the more reasonable result.

B. Integration with Enforcement Standards

Despite recent frenetic activity surrounding corporate governance issues,[61] the current federal organizational sentencing guidelines actually were established by the Sentencing Reform Act of 1991[62] (Sentencing Guidelines). These guidelines offer a business the possibility of reduced fines or penalties for wrongdoing if it can demonstrate it has diligently designed and implemented an effective compliance program. The Sentencing Guidelines attempt to set the tone in corporate America for dealing with governance issues related to legal and ethical compliance.[63]

Unfortunately, there is no apparent guidance addressing how a business should implement compliance programs for laws that are vague or ambiguous when applied.[64] Counsel advising these businesses are without consistent direction not only on how to protect their clients but, in light of recent developments surrounding ethical rules for lawyers, how to protect themselves. On August 12, 2003, the American Bar Association adopted proposed revisions to the *Model Rules of Professional Conduct* that include obligations for a lawyer to report potential illegal activity to higher authorities within a client organization and potentially outside that organization.[65] Such an obligation may apply if the lawyer knows facts from which a reasonable lawyer under the same circumstances would conclude that an organizational representative intends to violate a legal obligation to the organization or a law that could lead to substantial injury to the organization.[66]

The adoption of a rational and consistent framework such as the Absurdity Avoidance approach provides an objective, good-faith process to which businesses and their counsel can point as evidence of due diligence when designing and implementing compliance programs.

C. Other Approaches to Statutory Interpretation

Uniform principles or rules on statutory interpretation or, as suggested by Nicholas Rosenkranz in a recent article,[67] the adoption of a set of federal rules of statutory interpretation,[68] may provide much-needed guidance for Congress and the courts. These rules, however, are unlikely to be as helpful to businesses that are subject to compliance obligations imposed by statutes and regulations. Even if such rules were to prove helpful for compliance purposes, agreement on these principles or even agreement that uniform rules should be adopted is years away. Meanwhile, laws continue to be enacted and enforced and businesses and their counsel continue to face daily compliance decisions that cannot be postponed.

The current debate around statutory interpretation issues is lively and diverse,[69] but is largely directed at the courts and Congress.[70] In his article, Rosenkranz suggests that Congress adopt federal rules of statutory interpretation much akin to those that exist for civil procedure or evidence. He argues persuasively that, in most cases, Congress has the constitutional power to prescribe definitions, canons of interpretation, and the impact of legislative history on subsequent interpretations of its legislation. Furthermore, he suggests that this prescription is desirable given the lack of any "generally accepted and consistently applied theory of statutory interpretation."[71]

In each instance, whether the solution proffered is directed at Congress or at the courts, the target audience has the discretion to make interpretative decisions. In drafting legislation, Congress on the front end has the discretion to define and interpret,[72] or require certain interpretations, as it sees fit, subject to constitutional limitations and few reprisals.[73] On the "back end," courts may use judicial discretion and the facts of the case at issue to interpret a statute or regulation for which more than one possible interpretation exists, and sometimes when it does not.

Those businesses that must comply with the adopted text of a statute or regulation are caught square in the middle, insofar as they are without either authority or discretion. If they guess wrong, civil and criminal penalties can apply.[74] Moreover, the negative effects on public relations that often follow prosecution or just an investigation are arguably worse than the statutory penalties.

Existing rules and canons of interpretation that may offer tools for courts and legislators offer little to businesses interpreting statutes or regulations for compliance purposes. Compliance is a high-risk proposition and it is in a business' interest to document its interpretations in detail. The Absurdity Avoidance approach set forth in this Article is designed to provide guidance for these businesses and their counsel. It suggests a largely objective standard for statutory and regulatory interpretation for compliance purposes.

IV. Selected Privacy Rule Interpretation Issues

A. Other Health Plans

Employers sponsor certain Health Plans that do not fit neatly into the categories of self-insured or fully-insured, as those terms are used in the Rule. This causes conflicting interpretations of the application of the Privacy Rule in the industry. Two of the most

common conflicting interpretations involve healthcare FSAs and certain EAPs.[75] In addition, DHHS guidance appears inconsistent with respect to the application of the "other health plans" Catchall Category to employer plans and programs.[76] It is unclear whether an employer plan or program that falls into the Catchall Category, but is not a Group Health Plan, is subject to the Rule.

While DHHS issued subsequent guidance clarifying the Rule's application to the healthcare FSA,[77] no guidance has been issued with respect to EAPs, and the guidance with respect to FSAs, although instructive, remains incomplete.

1. Insured vs. Self-Insured

The definition of insurance, when used to determine which entities will be subject to state regulation as insurance companies, is a complex analysis that is beyond the scope of this Article. The generally accepted, as opposed to technical, meaning in the employer health plan context relates to the use of the terms "insured" and "self-insured" as applied to Group Health Plans. Insured employer plans are those plans for which the risk of the ultimate cost of the benefit is borne and paid by a third party in exchange for a set premium. A self-insured plan is one for which the employer or other sponsor ultimately bears the risk for, and pays, the costs of providing the benefits. Self-insured employer plans may be administered through a TPA, which processes and pays the claims, but the TPA is reimbursed by the employer for the costs of those claims and is usually paid an administrative fee for the TPA services. Some Group Health Plans may be a combination of insured and self-insured.

The Privacy Rule uses the terms "insured" and "self-insured" in its definition of Group Health Plans to indicate that the Rule applies to both categories of employer health plans.[78] The Rule neither references nor admits to the existence of any Group Health Plans that are neither insured or self-insured. As discussed, the Rule has significantly reduced compliance requirements for employer plans for which benefits are fully-insured by an insurance issuer or HMO. Moreover, the Rule carefully defines both "insurance issuer"[79] and "HMO,"[80] leaving no doubt that these terms refer to entities that are licensed by states as insurance companies, health maintenance organizations, or other similar entities that are regulated for solvency.

In the Rule's preamble, DHHS appears to use the term "insured" or "fully-insured" to refer to these plans for which the benefits are fully-insured by an insurance issuer or HMO. The reasoning provided for substantially exempting these plans from the Rule's

requirements in cases in which the insurance issuer or HMO does not disclose any protected health information to the Group Health Plan or to the sponsor is that insurance issuers and HMOs themselves are covered entities under the Privacy Rule. Thus, they are already subject to the requirements of the Rule.[81] To the extent that the only party that will use or disclose protected health information on behalf of the plan is already subject to the Rule, imposition of the Rule's requirements on the plan itself makes little sense. Moreover, for benefits provided fully by an insurance issuer or HMO, employees enroll directly with the insurance issuer or HMO, creating contractual privity and an obligation between those entities and the individuals whose information they handle.

It appears that DHHS fails to recognize, however, that there are employer health plans that do not fit neatly into either definition—fully-insured or self-insured—and are not "insured" at all. Specifically, certain plans, such as healthcare FSAs, certain EAPs, smoking cessation programs, and wellness programs, offer benefits for which the employer bears no financial risk and that are typically not fully-insured by an insurance issuer or HMO. Thus, the extent of the Rule's application to these plans is unclear.

2. Healthcare FSAs

A healthcare FSA is different from other Group Health Plans because it does not provide traditional insurance benefits. Employees designate an amount of money, up to an annual cap, to pay for healthcare that is not covered by other plans. This amount is deducted from that employee's salary, usually in equal installments throughout the year. The total amount, however, is available throughout the year for reimbursement to the employee for these noncovered healthcare expenses. The employee does not receive this FSA amount as income and does not pay income taxes on it. The amount set aside is available on a "use it or lose it" basis; any excess at the end of the year reverts to the employer. The employer pays the cost of administering this benefit and technically provides the funds for the medical care but has no additional out-of-pocket costs or other financial risk for the medical care.

A healthcare FSA qualifies as a Group Health Plan because it meets the definition of an employee welfare benefit plan under ERISA.[82] The healthcare FSA is often one benefit among others, such as a dependent-care FSA. In some cases, an employer "wrap-around" plan includes the FSAs and other benefit plans in one ERISA filing, and this filing may combine both Health Plans and Excepted Benefits. Whether and how the wrap-around plan structure affects Privacy Rule compliance is unsettled.[83] Whether structured

as a separate Covered Entity or as the healthcare component of a hybrid entity, the FSA clearly is subject to the full spectrum of compliance requirements under the Privacy Rule. This is true unless the FSA meets the definition of providing or paying the cost of an Excepted Benefit.

In addition, if a sponsor intends to receive any protected health information with respect to its healthcare FSA,[84] it will need to comply with and certify compliance with the Sponsor Requirements. Most plan sponsors currently receive protected health information with respect to their FSAs, if only in the form of debit reports. While these reports may contain only names and dollar amounts, they nevertheless meet the definition of protected health information because they identify the individual and relate to payment for the provision of healthcare. Any use or disclosure of protected health information by or on behalf of a covered entity implicates the Privacy Rule, and the reports fail to meet the definition of summary health information or enrollment or disenrollment information. Thus, a sponsor's receipt of these reports involves a disclosure of protected health information that will trigger the Sponsor Requirements.

While a healthcare FSA is not listed in the Privacy Rule as an Excepted Benefit, in a limited context it was found to qualify as an excepted benefit under the same overall section of the PHS Act that includes Excepted Benefits. The Internal Revenue Service, the Department of Labor (DOL), and DHHS issued a notice on December 29, 1997, stating that for purposes of applying the HIPAA rules with regard to pre-existing conditions under both the Internal Revenue Code and ERISA, excepted benefits included healthcare FSAs.[85]

The unusual nature of the FSA benefit and the classification of the FSA as excepted from other portions of HIPAA led lawyers and their clients initially to believe that the FSA may qualify as an Excepted Benefit under the Privacy Rule. Most healthcare FSAs qualify as small health plans under the Rule, pushing their compliance date to April 14, 2004. Thus, taking a "wait-and-see" attitude with respect to these small plans posed little risk to employers. In sparsely worded guidance issued on April 24, 2003, DHHS confirmed that healthcare FSAs are subject to the Privacy Rule.

> A "group health plan" is a covered entity under the Privacy Rule and the other HIPAA, Title II, Administrative Simplification standards. A "group health plan" is defined as an "employee welfare benefit plan," as that term is defined by the Employee

> Retirement Income Security Act (ERISA), to the extent that the plan provides medical care. . . . Thus, to the extent that a flexible spending account or a cafeteria plan meets the definition of an employee welfare benefit plan under ERISA and pays for medical care, it is a group health plan, unless it has fewer than 50 participants and is self-administered. Employee welfare benefit plans with fewer than 50 participants and that are self-administered are not group health plans. Flexible spending accounts and cafeteria plans are not excluded from the definition of "health plan" as excepted benefits.[86]

While the DHHS guidance provided little explanation, its conclusion is consistent with a more detailed analysis of whether the FSA is an Excepted Benefit.

The reasoning underlying the prior determination that FSAs were excepted benefits for purposes of defining pre-existing conditions does not easily extend to the Privacy Rule application. The December 29, 1997, notice determined that certain healthcare FSAs should be included in the excepted benefits identified under Section 2791(c) of the PHS Act. The Privacy Rule defines Excepted Benefits as only those listed under Section 2791(c)(1) of that act. In earlier guidance unrelated to the FSA issue, The Centers for Medicare & Medicaid Services (CMS) noted that the excepted benefits as defined in Section 2971(c)(2) of the act, such as limited scope dental or vision benefits, were not explicitly excepted from the Rule and could be considered Health Plans. CMS explained that "such plans, unlike the programs and plans listed at Section 2971(c)(1), directly and exclusively provide health insurance, even if limited in scope."[87]

A healthcare FSA directly and exclusively pays for the cost of Medical Care. It does not, however, provide what is typically identified as health insurance, because no financial risk-bearing is involved. The implied principle that the benefit provided is primarily for Medical Care purposes is a generally consistent distinction between the health plans that are covered by the Rule and those that are Excepted Benefits.[88] Disability insurance, worker's compensation, and, to some extent, life insurance, are primarily to compensate a person for lost income or other expenses incurred because of death, injury, or disability. Their primary purpose is not to pay for Medical Care. Even though all or part of the money derived from those benefits may be used by beneficiaries for that purpose and, with respect to worker's compensation benefits, may be calculated

partially on the basis of those expenses, the programs are not purposed on dollar-for-dollar reimbursement for those expenses.

This reasoning is consistent with the Rule's application to Group Health Plans "to the extent that the plan provides [M]edical [C]are" through insurance, reimbursement, or otherwise.[89] The FSA is an ERISA plan. Thus, if it does not provide an Excepted Benefit, it is subject to the Rule to the extent it provides Medical Care through insurance, reimbursement, or otherwise. The healthcare FSA provides Medical Care through reimbursement, and this reimbursement for Medical Care is its primary purpose.

What the DHHS guidance does not clarify, however, is how the healthcare FSA is regulated under the Rule. The FSA does not fit neatly into the category of either insured or self-insured plan as those terms are used in the Rule.

3. Employee Assistance Programs

Many employers offer their employees an EAP. Although some disagreement exists on whether and to what extent EAPs are Group Health Plans, the DOL has issued at least one opinion holding that an EAP which provided counseling qualifies as an ERISA plan.[90] The DOL concluded that an EAP under which coverage was provided for services addressing mental or physical health was an employee welfare benefit plan because the program provided "benefits in the event of sickness." The letter noted that ERISA Section 3(1) defines the term employee welfare benefit plan as:

> any plan, fund or program . . . established or maintained by an employer . . . to the extent that such . . . was established or is maintained for the purpose of providing for its participants or their beneficiaries, through the purchase of insurance or otherwise, (A) medical, surgical, or hospital care or benefits, or benefits in the event of sickness, accident, disability, death or unemployment, or vacation benefits.[91]

While some EAPs are solely referral services, many provide several counseling sessions before referring an employee to a third-party provider. A distinction between EAPs that provide less than three or four counseling sessions and those that provide more than three or four sessions has been adopted by some benefits consultants and organizations as the benchmark for determining whether an EAP is a welfare benefit plan under ERISA. This distinction does not appear to be based on any official judicial or governmental opinion or pronouncement.

In many cases, the counseling and referral functions are provided by a third-party EAP services entity that is not a licensed insurance issuer or HMO. Such entities are not themselves subject to the Privacy Rule.[92] Moreover, the benefits commonly are provided on behalf of employers for a set per-member per-month charge. In other words, an employer pays the set fee each month for each employee, whether or not and to whatever extent the employee uses the benefit. This payment methodology transfers the risk of the ultimate cost of providing the benefit to the EAP services entity because the employer's costs are fixed, yet the extent of services that will be required to be provided each month is uncertain.

Some confusion exists concerning the application of the Privacy Rule to plans for which benefits are provided by an insurance issuer or HMO. This results from the Rule's use of the term "insured" and the reasonable interpretation that EAPs that function on the per-member per-month model are more akin to insured rather than self-insured plans. Some employers have concluded that the plans fit the definition of insured plans. As such, as long as the employer as sponsor receives no protected health information from the EAP services entity, the EAPs are exempt from the requirements of the Privacy Rule as if the benefits were provided by an insurance issuer or HMO.

Thus, at issue is whether an EAP is a Health Plan and whether it is subject to the full spectrum of compliance requirements imposed on self-insured plans.

4. Catchall Category Plans

Employers sponsor a variety of other plans or programs that provide or pay for the cost of Medical Care. These plans appear to be plans captured by the Catchall Category in the definition of Health Plans. Programs such as smoking cessation programs, wellness programs, health fairs, free flu vaccines, and the like (collectively, Other Programs) may or may not be Group Health Plans under ERISA. To the extent these Other Programs are ERISA plans, the issue becomes, as with FSAs or EAPs, whether they are to be regulated as an insured or self-insured plan under the Rule. None of these Other Programs fit well within the definition of either an insured or self-insured plan. To the extent any of these Other Programs are not ERISA plans, the question raised is whether they are subject to the Rule under the Catchall Category or not subject to the Rule at all.

While the definition of a Health Plan under the Rule and the definition of an ERISA plan are similar, they are not identical.[93] The Rule

provides no guidance as to whether a plan or program that is paid for by an organization for its employees and is not a Group Health Plan but meets the Catchall Category definition was intended to be captured by that definition.

In the preamble to the Rule and in response to a public comment asking whether employer discount programs, membership incentive programs, and other "unfunded" employee benefits are Health Plans, DHHS replied that:

> Only those special employee discounts or membership incentives that are "employee welfare benefit plans" . . . and provide "medical care" . . . are health plans for the purposes of this rule. Discount or membership incentive programs that are not group health plans are not covered by the rule.[94]

This comment admittedly supports the proposition that only employee benefits that qualify as ERISA plans are Health Plans. That support is weakened, however, by the nature of the discount programs and membership incentives that are the subject of the comment, the absence of a reference to the Catchall Category in the reply, and the broad language elsewhere with respect to the Catchall Category.

Discount programs, membership incentive programs, and other "unfunded" benefits for which no cost is incurred by the employer, and that usually are offered to organizations by vendors as a marketing effort, do not meet the definition of Health Plan for other reasons. Specifically, those programs do not involve the employer providing or paying the cost of Medical Care. Rather, they simply involve the employer giving access to vendors who have agreed to offer employees a discount or incentive. Thus, these programs are not akin to the Other Programs at issue in this discussion.

A public comment urged the DHHS Secretary to clarify that the Catchall Category includes "24-hour coverage plans" that integrate traditional employee health benefits with workers compensation coverage. In response to this comment, DHHS clarified "that to the extent that the 24-hour coverage plans have a health care component that meets the definition of 'health plan' in the final rule, such component must abide by the provisions of the final rule."[95] This response is ambiguous because even though the question references the Catchall Category, the response does not because the healthcare portion of a 24-hour coverage plan is an ERISA plan that otherwise meets the definition of a Health Plan.

Finally, in the preamble, DHHS responded to public comments asking the DHHS Secretary to clarify the Catchall Category and to specify which plans would meet the criteria for this category:

> This statutory language is general, not specific, and as such, we are leaving it general in the final rule. However, as described above, we add explicit language which excludes certain "excepted benefits" from the definition of "health plan" in an effort to clarify which plans are not health plans for the purposes of this rule. Therefore, to the extent that a certain benefits plan or program otherwise meets the definition of "health plan" and is not explicitly excepted, that program or plan is considered a "health plan" under . . . the final rule.[96]

This comment implies that benefit plans other than Group Health Plans are Health Plans if they are not Excepted Benefits and they satisfy the Catchall Category definition.

B. Enrollee Authorizations

The Privacy Rule provides that a covered entity may use or disclose protected health information pursuant to and in compliance with an authorization signed by the individual to whom the protected health information relates or the individual's personal representative.[97] Authorizations under the Rule are valid if they meet a set of requirements that includes a prohibition on a covered entity conditioning the provision of treatment, payment, enrollment, or eligibility for benefits on the provision of an authorization.[98] Other than this prohibition and specific content requirements, the Rule imposes no specific limits on the use of authorizations.[99]

For self-insured Group Health Plans, often the only protected health information an employer or sponsor receives is the information necessary to hear final appeals on denials of claims. This final appeals adjudication is the sponsor's role as the ERISA plan fiduciary. A sponsor may contractually transfer this fiduciary responsibility to the plan TPA, but many TPAs will not agree to assume the duty and associated liability. Moreover, because the sponsor of a self-insured plan is the party that ultimately will pay the costs of all approved claims, many sponsors are reluctant to transfer this adjudication authority to a third party that has no financial stake in the decision.

Claims are rarely appealed to the fiduciary. To avoid the Sponsor Requirements imposed by the Privacy Rule, some sponsors have

adopted the use of enrollee authorizations as a way to gain access to the necessary protected health information on an ad hoc basis for final appeals.[100] These sponsors avoid receiving protected health information for any other purpose and represent to plan enrollees that they do not use or disclose protected health information without individual authorization.[101] If or when an enrollee appeals a claim denial to the plan fiduciary, the sponsor requires the enrollee to sign an authorization allowing disclosure to the sponsor of the protected health information necessary for the sponsor to decide the appeal.

Some sponsors have adopted a policy of obtaining employee authorizations for the use of Group Health Plan data for the administration of other benefit plans, such as disability plans. This is a use that otherwise is prohibited by the Privacy Rule.[102] Generally, an employer must obtain protected health information directly from the affected employee or his physician for purposes of disability benefit plans, which themselves are not covered entities under the Rule. When the information is disclosed by the physician, an authorization under the Privacy Rule is required for the physician to be able to disclose the information. This authorization may be required by the sponsor as a condition to access disability benefits. This falls under the specific exception in the Rule for cases in which the treatment or benefit is for the sole purpose of creating protected health information for disclosure to a third party, such as pre-employment and disability physicals.

While not obvious, a distinction can be made between: (1) requiring an employee to sign an authorization that allows an employer to use the employee's protected health information from a disability physical for purposes of a disability benefit determination; and (2) requiring an employee to sign an authorization that allows the disability plan, for purposes of that disability benefit determination, to access all the employee's protected health information maintained by the employer's Health Plan. In the second case, the authorization would allow access to a much broader category of information. This information may be related to prior or separate treatment by other providers and may be used by the employer to contradict or interpret the information provided by the physician who is selected by the employee or employer for the disability determination. In addition, the authorization in the second case does not appear to meet the specific exception in the Rule for cases in which the treatment or benefit being conditioned is for the sole purpose of creating the protected health information for disclosure to the third party. In the case of the broader Health Plan authorization, the provided treatment was

almost certainly for a purpose other than disclosure to a third party for the disability determination.

At issue is the prohibition on conditioning payment or eligibility for benefits on the provision of an authorization, and whether this prohibition prevents the use of authorizations in the two types of situations discussed below.

V. Analysis and Conclusions

A. Other Health Plans

This section applies the Absurdity Avoidance analysis to two issues left unclear in the Privacy Rule with respect to the FSA and EAP plans. These analyses illustrate the importance, in the context of compliance, of following the prongs of the approach in order. The first analysis is whether the EAP is a Health Plan under the Privacy Rule. The second analysis is whether the FSA and/or EAP should be treated by employers as self-insured or fully-insured plans. The analysis also addresses whether the Catchall Category applies to all employer programs or only those employer programs that are Group Health Plans.

The results of these analyses also apply to the Other Programs that provide or pay the cost of Medical Care but do not fit neatly into the insured or self-insured category.

1. Whether an EAP is a Health Plan

The Textual Test indicates that an EAP which provides counseling is a Health Plan because it is an ERISA plan that provides Medical Care.[103] This conclusion is supported by a DOL opinion rather than judicial ruling and possibly could be subject to legal challenge. The conclusion, however, is consistent with the definition of an ERISA plan and appears to be accurate. An EAP that does not provide counseling but simply consists of a referral hotline has been found not to be an ERISA plan. Thus, such an EAP is not a Health Plan unless it meets another part of the Health Plan definition.

As noted, the only other aspect of the definition that could be applicable is the Catchall Category of "other plan or program" that provides or pays the cost of Medical Care. Medical Care is broadly defined. From a purely textual perspective, it is not certain that a hotline, through which someone listens to a caller's problems and recommends a resource, could never be found to be a service that mitigates or prevents disease or effects any structure or function of the body.[104]

The Commentary Test reveals no specific government guidance on the EAP, but related guidance is relevant. The OCR guidance that provided FSAs are Health Plans because they are ERISA plans,[105] and the absence of any relevant contrary guidance, supports the result of the Textual Test that the EAP providing counseling is indeed a Health Plan. No reasonable argument to the contrary appears to exist. Thus, the application of the first two tests produces a result sufficiently clear to end the inquiry.

As discussed, contradictory DHHS guidance exists that categorizes an EAP hotline, which is not an ERISA plan, as a Health Plan. DHHS categorized EAP hotlines in this way because they fit the Catchall Category. An EAP hotline is a service for which an employer pays. As such, it does not fall into the category of examples listed in the DHHS guidance that excepts discount programs and the like.[106] Its status as a non-ERISA plan that makes the commentary potentially applicable is, however, contradicted by the commentary with respect to the Catchall Category. While it may not be unreasonable to determine the EAP hotline is not a Health Plan, based on the tenuous application of the Catchall Category, an argument still exists that it could be a Health Plan. When any arguable doubt exists, proceeding with the remaining two tests is indicated, particularly given that the application of those tests does not require much in the way of time or resources.

The Purposes Analysis first requires the identification of the purpose or purposes of the statute or regulation at issue. The Privacy Rule implements portions of the administrative simplification provisions of HIPAA that relate to a person's individually identifiable health information.[107] Section 264 of HIPAA provides that the Secretary of DHHS shall recommend standards with respect to the privacy of individually identifiable health information that would address at least the following: the rights that an individual should have with respect to his or her individually identifiable health information; the procedures that should be established to exercise those rights; and the uses and disclosures of that information that should be authorized or required.

The administrative simplification provisions of HIPAA were enacted to improve the efficiency and effectiveness of the healthcare system by encouraging the development of a health information system.[108] DHHS established standards and requirements for the electronic transmission of certain health information to facilitate such a system.[109] It identified three major purposes for the Privacy Rule: (1) to protect and enhance consumer rights to access and control inappropriate use of their health information; (2) to restore

trust in the healthcare system; and (3) to improve the efficiency and effectiveness of that system through the establishment of a national framework for health privacy protection.[110] The DHHS Secretary also noted that the Rule "seeks to balance the needs of the individual with the needs of society."[111] The DHHS Secretary explained in detail the "legitimacy of various uses and disclosure of health information,"[112] the necessary "balance between the burden on covered entities and need to protect privacy,"[113] and the need to achieve that balance "in a way that is also workable for the varied stakeholders"[114] and "track[s] current practices."[115] The purposes of the Privacy Rule involve a balancing of the competing interests of individual privacy and societal needs. As such, the Purposes Analysis is less determinative of the overall outcome of the Absurdity Avoidance framework but, nonetheless, is still significant.

If an EAP hotline were found to be a Health Plan, the protected health information that would be subject to the Rule's protections would be the name of the callers, any details concerning the problems for which the call was made, and any referrals to a third-party resource provided by the hotline. If the hotline were not a Health Plan, in the absence of applicable state law, this information would not be subject to any consistent protection or restrictions on use and disclosure. Protecting that information at first blush seems consistent with the purpose of protecting individual privacy. Most EAP hotlines, however, currently cost employers little and operate in a way that employers are never provided the identity of callers. In fact, many times the caller's identity is not requested by or required to be disclosed to the hotline. Ironically, imposition of the Rule's compliance requirements would increase the likelihood of disclosure of the information to employers if employers were responsible for hotlines' compliance with the Rule.

Trying to determine which entity would be responsible for the program's compliance provides the line of analysis that, under the Absurdity Analysis, finally clarifies the result produced by the application of the four tests. These EAP hotlines do not meet the definition of a Group Health Plan under ERISA. Thus, if they are Health Plans, it is unclear who is responsible for the programs' compliance with the Rule or the role of the employer. The employer would not be a sponsor because that role is defined in the Rule solely in terms of the ERISA plan definition.[116] The employer is paying for the program, but the program is administered by a third party. The program itself is not a separate legal entity, as is the case with an ERISA plan. Thus, it is unclear what entity is the "Covered Entity."

If the program is a Health Plan, some legal entity must be a Covered Entity or a hybrid entity. It makes no sense to designate the hotline provider as the Covered Entity because the hotline provider is not providing or paying for the cost of the benefit and, thus, by definition does not meet the definition of a Health Plan unless one argues that bearing the risk under a per-member, per-month payment scheme qualifies. In any event, that argument fails because the hotline provider, like other EAP service providers, is not an individual or group plan or program because it has no contractual privity with or obligation to any individual or group. Its contractual privity is with the employer or the employer's plan. The beneficiaries of its services derive the benefit from the employer plan, and the obligation to provide the benefit to the beneficiary rests with the employer plan. Thus, the hotline provider is a service provider to the covered entity plan and not a Health Plan in its own right. If the employer is the Covered Entity, then by definition any employer offering an EAP hotline automatically becomes a Covered Entity subject to the Privacy Rule, another absurd result.

Finally, the interpretation that the EAP hotline is not a Health Plan, and that any other employer program that does not meet the definition of a Group Health Plan under ERISA is not a Health Plan, is not an absurd result. These programs are small benefits that do not cost an employer great sums, participation by employees is voluntary, and burdening the programs with substantial compliance requirements is likely to discourage their availability. The inconsistency in protecting an employee's health information with respect to Group Health Plans and not with respect to these benefits that are not Group Health Plan benefits is not an inconsistency in the context of the Rule. The Rule excepts from its reach many programs, such as disability plans and pre-employment physicals, through which an employer collects employee health information.

In summary, with respect to EAPs that provide counseling and are Group Health Plans, the Textual Test provides a clear result that those plans are subject to the Rule. This result is supported by the Commentary Test. With the EAP hotlines, the Textual Test provides no guidance on the issue and the Commentary Test offers conflicting support as to whether employer programs that are not Group Health Plans can be subject to the Rule under the Catchall Category. One could argue both ways as well with the Purposes Analysis. When the application of each interpretation undergoes the Absurdity Analysis, however, the interpretation that these programs are subject to the Rule as covered entities produces an absurd result. The exception of these programs from regulation under

the Rule produces a result that is not absurd. Thus, for compliance purposes, it seems reasonable for businesses and their counsel to determine that these programs that are not Group Health Plans are not Health Plans subject to the Rule.

2. Regulation of FSAs and EAPs

The next step is to apply the Absurdity Analysis to the issue of whether the FSA and EAP, and other non-traditional Group Health Plans, are subject to regulation by the Rule as insured or self-insured plans. Under the Textual Test, if the employer contracts with an insurance issuer or HMO to fully insure the plan benefits, then the plans meet the definition, and the insured exemption may be applied. While it is not the norm, it is possible to contract with an insurance issuer or HMO to fully insure an EAP program. This is anathema to an FSA, however, because the benefits are never insured, but rather are paid for by the money set aside from the employee's defined salary. Thus, only a small subset of these two types of plans meet the textual definition of insured.

Applying the Textual Test with respect to the self-insured category is more complex because the Rule does not provide a specific definition for this term or category of plans. The Rule's use of the term "self-insured" fails to shed any light on the issue, but is not inconsistent with the inclusion of the FSA or the EAP in the case in which the benefit is not insured by an insurance issuer or HMO. Thus, for this category of plans, the Textual Test provides no direction.

For the small subset of EAPs for which the benefit is fully-insured by an insurance issuer or HMO and for which the Textual Test provides a clear result, application of the Commentary Test supports that result[117] and concludes the analysis. For the remainder of EAPs and all FSAs, the Commentary Test provides no additional information. As such, the Textual Test and Commentary Test each support the conclusion that these EAPs and FSAs do not meet the definition of insured plans under the Rule and that determination may be made with confidence. These first two tests are not inconsistent with the determination that these plans are self-insured, but they provide no real support for that conclusion other than it appears to be the only choice remaining.

While the inquiry could stop at this point, the absence of another good option is more of a subjective determination than an objective application of the Textual and Commentary Tests. As such, it is more appropriate for the second set of tests. Also, the Rule may simply not have contemplated these unique plans and, thus, failed to provide an appropriate regulatory structure for them.

It is not unreasonable, therefore, to continue with the analysis. The Purposes Analysis provides minimal additional assistance. It is consistent with the purposes of the Rule for these plans to be Health Plans and placed into a category of Health Plans for which regulatory requirements are provided. Consequently, a conclusion that these EAPs and FSAs are to be regulated as self-insured plans is consistent with the Rule's purposes. Alternatively, to conclude that the plans were neglected by the drafters of the Rule and pose an issue that requires promulgation of additional regulations is hardly inconsistent with the Rule's purposes. Those purposes, however, may be frustrated during the waiting period for further regulation or guidance.

The Absurdity Analysis in this case produces a result less than satisfying, but the result is practical. If the EAPs that are not insured by an insurance issuer or HMO and the FSAs are regulated as self-insured plans, then they are subject to the full panoply of Health Plan Requirements. If the sponsor receives any protected health information in administering these plans, which is usual for FSAs, then those sponsors are subject to the Sponsor Requirements as well. This is not an absurd result judged under the proposed standard—notwithstanding the fact that the cost of compliance may far outweigh the cost of providing the underlying benefit.

Further, the exception of these EAPs and FSAs from any regulation under the Privacy Rule produces a result that makes little sense and could be termed absurd. Employers may not receive much health information in the provision of the FSA or EAP because in most cases claims are administered by a TPA and claims level detail is not provided to the employer. The health information received and used by the TPA, however, is similar to that received and used by other Group Health Plans. Such information concerns Medical Care that typically is prescribed by a physician and not voluntarily accessed in the same sense that participating in a free flu-vaccine program is voluntary. If the TPA is not an insurance issuer or HMO, the Rule would not apply to its activities if not through its application to the FSA or EAP as a self-insured plan. If these FSAs or EAPs are not subject to the Privacy Rule, the information will receive protection when the claims are submitted for reimbursement by traditional insurance and not receive protection for purposes of FSA reimbursement. This is a difference with no apparent justification. Thus, these plans should be regulated as self-insured plans.

The result may not be completely satisfying because it does not take into account what could truly be the case—that the Rule's drafters neglected to consider these unique plans and their differences from typical Group Health Plans and that special rules

would have been developed to deal with those differences. While this reasoning is attractive, it borders on the absurd to expect a business to decide not to comply with the Rule with respect to its FSA or EAP for that reason.

In summary, with respect to EAPs that are fully insured by an insurance issuer or HMO, the Textual Test produces a clear result supported by the Commentary Test, which settles the issue. With respect to other FSAs and EAPs, and other nontraditional programs that are Group Health Plans and are regulated under the Rule, neither the Textual Test nor the Commentary Test provides any direction. The Purposes Analysis produces an inconclusive result. The Absurdity Analysis, however, highlights and supports the judgment issues apparent from the beginning: (1) it makes no sense for these plans not to be regulated because they clearly are Group Health Plans subject to the Rule; (2) they are clearly not fully-insured by an insurance issuer or HMO; and (3) to regulate them as self-insured plans, though perhaps burdensome, is not an absurd result.

B. Enrollee Authorizations

Two issues concerning whether an employer may utilize enrollee authorizations remain unclear under the Privacy Rule. First, it is unclear whether enrollee authorizations may be used rather than implementing the full panoply of Sponsor Requirements for gaining access to protected health information in the rare cases of final appeals of denials of benefits. Second, it is unclear whether their use is proper when using Health Plan data in administering other benefit plans, such as disability plans.

The Textual Test indicates the Rule provides that a covered entity may use and disclose protected health information with an authorization that provides for that use or disclosure. The only limitation is that a covered entity may not require an authorization as a condition to receiving treatment, payment, enrollment, or eligibility for benefits.[118] The Rule seems clear that access to the final appeal of an enrollee denial of benefits and, as a consequence, the benefits, may not be conditioned on the requirement that the enrollee sign an authorization. Instead, the sponsor must implement the Sponsor Requirements for access by the sponsor to protected health information. Similar reasoning does not apply to an employer requiring an employee to sign an authorization for access to Health Plan data as a condition of receiving a disability benefit. This is true because the employer is not a Covered Entity and is not acting on behalf of a Covered Entity when acting on behalf of the disability plan.

The disclosure of Health Plan data for use by the sponsor in administering other benefit plans that are not covered entities, such as disability plans, implicates another provision of the Rule. A sponsor that receives protected health information from a Group Health Plan for administration of that plan is prohibited from using that protected health information for any other plan or benefit.[119] Thus, the issue is whether a sponsor can circumvent this prohibition by obtaining specific authorization from the enrollee to allow the use or disclosure. The text of the Rule supports an employer's ability to do just that. Authorizations are for the purpose of authorizing otherwise prohibited uses and disclosures.[120]

While other laws may apply in the context of use of health information in determining disability, the Textual Test supports an employer's ability under the Privacy Rule to require and use an authorization in this circumstance. Moreover, the text also supports the ability of an employer to request a voluntary authorization for these purposes, which may blunt any criticism or other legal issues associated with an absolute requirement.

While not determinative, DHHS guidance is not inconsistent with the results obtained under the Textual Test for these issues. Policy reasons may exist, however, that support contrary results. One may argue that employees sign whatever employers provide to them to sign. Thus, the unequal bargaining positions create an unfair result. Employees may not realize the impact of authorizing the use of their Health Plan data for other benefit program purposes.

In addition, a persuasive argument exists that employers, as fiduciaries to all ERISA plans, may not decide when they are acting on behalf of one plan that is not a Covered Entity versus a plan that is a Covered Entity. This argument, however, is neither based on nor supported by the Privacy Rule, which clearly provides for a sponsor to wear two hats—sponsor and employer. It also clearly provides that an employer acting as an employer may use authorizations to obtain protected health information. For instance, an employer may assist an employee in investigating a claim submitted to a fully-insured plan from which the sponsor otherwise receives no protected health information. Other laws may affect the outcome in any given case. The textual and commentary support for these issues is not ambiguous with respect to the Privacy Rule's impact. The inquiry under the Rule ends at this point.

In summary, the Textual Test and Commentary Test are clear and consistent in producing a result that an employer may use an employee authorization to access protected health information about

that employee for use in making a determination with respect to another plan or benefit.

VI. Conclusion

The absence of a rational framework for making statutory and regulatory interpretation decisions for compliance purposes leads to inconsistent interpretations that are difficult to support when questioned by government authorities or the courts. This is especially true in light of the contrary clarity that hindsight often produces. The application of the Privacy Rule to employer Health Plans provides a good example of the myriad of compliance decisions that must be made by businesses and their counsel in the face of unclear statutory or regulatory guidance.

The Absurdity Avoidance framework proffered in this Article provides a rational, practical framework to use with respect to the Privacy Rule and other statutes and regulations for which compliance interpretations are required. The application of the framework can be documented and provides a solid basis to support decisions made in good faith in the context of the time and circumstances in which they were made.

Endnotes

[1] Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462 (Dec. 28, 2000).

[2] Health Insurance Portability and Accountability Act (HIPAA) of 1996, Pub. L. No. 104-191, 110 Stat. 1936. The Privacy Rule is one of a set of regulations mandated under title II, subtitle F, §§ 261-264 of HIPAA, and titled "Recommendations with Respect to Privacy of Certain Health Information."

[3] *See* Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462, 82,472 (Dec. 28, 2000) (to be codified at 45 C.F.R. pts. 160, 164) ("The Secretary has decided to delegate her responsibility under these regulations to the Department's Office for Civil Rights.").

[4] Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. at 82,472; 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); 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); Dep't of Health and Human Servs., *Office for Civil Rights—HIPAA: Medical Privacy—National Standards to Protect the Privacy for Personal Health Information*, *at* www.hhs.gov/ocr/hipaa/ (last visited Apr. 5, 2004).

[5] Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. at 82,472.

[6] Dale Carpenter, *Keeping Secrets,* 86 Minn. L. Rev. 1097, 1110-11 (2002).

[7] 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, 1470 (2002).

[8] Peter D. Jacobson, *Medical Records and HIPAA: Is It Too Late To Protect Privacy?*, 86 Minn. L. Rev. 1497, 1499 (2002).

[9] 29 U.S.C. § 1002(1) (2004).

[10] Indeed, many other unsettled issues have arisen in the application of the Privacy Rule to employer group health plans, including: (1) whether sponsor workforces who provide plan administration functions for self-insured plans administered by third parties are subject to the health plan workforce compliance requirements, such as training, or only to the partially overlapping requirements specifically set forth in the Rule as applicable to plan sponsors performing plan administration functions; (2) whether employers with "wrap-around" plans must count all benefits under the wrap-around plan, which may include medical, dental, vision, cafeteria plans, and others, as one covered entity health plan for Privacy Rule compliance purposes; and (3) to what extent the state law preemption analysis under the Privacy Rule applies to Group Health Plans. These issues and others merit discussion but are beyond the scope of this Article. Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. at 82,508.

[11] HIPAA applies only to "covered entities," which are defined as (1) a health plan, (2) a healthcare clearinghouse, and (3) a healthcare provider who transmits any health information in electronic form in connection with a transaction governed by HIPAA. 45 C.F.R. § 160.103 (2004). The Privacy Rule governs uses and disclosures by Covered Entities of protected health information. The Rule provides certain rights for individuals with respect to their protected health information, and imposes certain administrative requirements on Covered Entities. *See generally* Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462.

[12] 45 C.F.R. § 160.104 (2004).

[13] *See id*. § 160.103.

[14] *See* Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. at 82,772.

[15] 42 U.S.C. § 300gg-91(a)(2) (2004).

[16] *See* 45 C.F.R. § 160.103 (2004). An employee welfare plan includes any plan, fund, or program that is established or maintained for the purpose of providing medical, surgical, or hospital care or benefits or benefits in the event of sickness.

[17] The Privacy Rule defines a Group Health Plan as:

> 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 the plan provides medical care (as defined in section 2791(a)(2) of the Public Health Service Act (PHS Act)) . . . to employees or their dependents directly or through insurance, reimbursement, or otherwise, [and that h]as 50 or more participants . . . or is administered by an entity other than the employer that sponsors the plan.

45 C.F.R. § 160.103 (2004) (defining Health Plan).

[18] *Id*. § 160.103 (including in the definition of Health Plan: HMOs, health insurance issuers, issuers of long term care policies (excluding nursing home fixed indemnity policies), certain government programs, and any other individual or group plan that provides or pays for the cost of medical care).

[19] *Id*. § 160.103 (excluding from the definition of Health Plan "[a]ny policy, plan or program to the extent it provides, or pays the cost of, excepted benefits listed in section 2791(c)(1) of the PHS Act, 42 U.S.C. § 300gg-91(c)(1).").

[20] *See* 42 U.S.C. § 300gg-91(a)(2) (2004). It is important to note that while on-site clinics are not health plans covered by the Privacy Rule, these clinics may be subject to the Rule as covered providers.

[21] *See* 45 C.F.R. § 160.103 (2004).

[22] *Id*. § 160.103. CMS has issued guidance on how to determine annual receipts for this purpose that in part provides:

> Health plans that do not report receipts to the IRS—for example, ERISA welfare plans that are exempt from filing income tax returns—should use proxy measures to determine their annual receipts. Fully insured health plans should use the amount of total premiums which they paid for health insurance benefits during the plan's last full fiscal year. Self-insured plans, both funded and unfunded, should use the total amount paid for health care claims by the employer, plan sponsor or benefit fund, as applicable, on behalf of the plan during the plan's last full fiscal year. Those plans that provide health benefits through a mix of purchased insurance and self-insurance should combine the proxy measures to determine their total annual receipts.

Ctrs. for Medicare and Medicaid Servs., "HIPAA 101" Video Script, May 12, 2003, *at* www.cms.hhs.gov/hipaa/hipaa2/education/May12videoscript.doc (last visited Apr. 5, 2004).

[23] 45 C.F.R. § 164.534(b)(2) (2004).

[24] *Id.* § 164.534(b)(1).

[25] Protected health information is defined in the Rule to mean individually identifiable health information that is transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form of medium, except for "(i) [e]ducation records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g; (ii) [r]ecords described at 20 U.S.C. 1232g(a)(4)(B)(iv); and (iii) [e]mployment records held by a covered entity in its role as employer." *See* 45 C.F.R. § 160.103 (2004).

[26] Except for uses and disclosures made pursuant to an authorization, disclosures made to a provider for treatment purposes, and certain other disclosures specified by the Rule, a covered entity may use or disclose only the minimum amount of protected health information necessary to accomplish the intended purpose. 45 C.F.R. §§ 164.502(b)-164.514(d) (2004).

[27] *See generally id.*

[28] *See id.* § 164.508.

[29] *See id.* § 164.520. "A [G]roup [H]ealth [P]lan that provides benefits solely through an insurance contract with a health insurance issuer or HMO and that creates or receives protected health information in addition to summary health information as defined in § 164.504(a)" or enrollment or disenrollment information must maintain its own notice, separate from the notice provided by the HMO or issuer, and provide it upon request to any person. The issuer or HMO is required to actually send its notice to enrollees as specified in the Rule. In most cases, compliance can be structured such that two separate notices are not required. Specifically, if the plan itself receives no protected health information but the HMO or issuer instead provides protected information to the sponsor to perform the administrative functions on behalf of the plan, then it need not comply with the notice and other requirements or the Rule, but must amend the plan documents and otherwise comply with the Privacy Rule requirements. *Id.* § 164.520.

[30] *See* 45 C.F.R. §§ 164.502(c)-164.504(e) (2004).

[31] *See id.* § 164.530(a)(1).

[32] *Id.* §§ 164.524-164.528.

[33] *See id.* § 164.530.

[34] The Rule provides that

> Summary health information means information . . . : (1) [t]hat summarizes the claims history, claims expenses, or type of claims experienced by individuals for whom a plan sponsor has provided health benefits under a [G]roup [H]ealth [P]lan; and (2) [f]rom which the identifiers described in § 164.514(b)(2)(i) have been deleted, except that the geographic identifier described in § 164.514(b)(2)(i)(B) need only be aggregated to the level of a five digit zip code.

Id. § 164.504(a). Essentially this definition requires that the information be de-identified except for the ZIP code and geographic subdivisions (*e.g.,* city) that are larger than the ZIP code.

[35] The Rule describes enrollment and disenrollment information as information on whether the individual is participating in the Group Health Plan, or is enrolled in or has disenrolled from a health insurance issuer or HMO offered by the plan. 45 C.F.R. § 164.530(k)(1).

[36] The Rule provides that in these circumstances the Group Health Plan is subject only to the requirements set forth in three subsections: (g) (refraining from intimidating or retaliatory acts against individuals exercising their rights under the Rule); (h) (refraining from conditioning benefits on a waiver of rights); and sometimes (j) (documentation requirements in the case of amendments to plan documents). *Id.* § 164.530(k)(2).

[37] *See generally* Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462, 82,627-28 (Dec. 28, 2000) (to be codified at 45 C.F.R. pts. 160, 164); Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. 53,182, 53,248 (Aug. 14, 2002) (to be codified at 45 C.F.R. pts. 160, 164). The contractual transfer of a Health Plan's obligations to a TPA is separate and apart from the Business Associate obligations a Health Plan is required to impose on certain third parties.

[38] The Rule requires that Group Health Plans require sponsors to comply with certain requirements as a condition of receiving protected health information from the plan. As a practical matter, for self-insured plans, the sponsor is the one who must ensure the plan's compliance with the Rule by requiring of itself compliance with the sponsor requirements. This circle is just one example of the conceptually confusing compliance structure created for employer health plans by the Privacy Rule.

[39] Civil money penalties for failure of a Covered Entity to comply with HIPAA regulations may be imposed in a fine of up to $100 for each violation, not to exceed $25,000 in any calendar year for violations of the same requirement. *See* 42 U.S.C. § 1320d-5 (2004). Criminal penalties for any person who knowingly obtains or discloses individually identifiable health information in violation of the HIPAA regulations start with fines of not more than $50,000 and imprisonment up to a year, or both, and can increase, depending on intent factors, up to a fine of not more than $250,000 and imprisonment up to ten years, or both. *See id.* § 1320d-6.

[40] Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. at 82,507. Throughout this discussion, when reference is made to disclosure of information by a Group Health Plan, that reference includes disclosure by an HMO or insurance issuer with respect to the Group Health Plan.

[41] *See* 45 C.F.R. § 164.504(a) (2004). Plan administration functions are defined in the Rule as administration functions performed by the plan sponsor on behalf of the Group Health Plan and exclude functions performed in connection with any other benefit or plan.

[42] *Id.* § 164.504(f)(2)(i).

[43] This is accomplished by providing a description of the workforce members or classes of workforce members who shall be given access to the enrollee protected health information and assurance that this access shall be restricted to the plan administration functions that the employer performs for the Health Plan. In addition, it requires a provision that describes a mechanism for resolving any issues of noncompliance by any workforce member or other person who is given access to enrollee protected health information. *Id.* § 164.504(f)(2)(iii).

[44] *Id.* § 164.504(f)(2)(ii) (discussing that in addition to amending the plan documents to provide these terms, the plan sponsor must also make this certification to the Health Plan).

[45] *Id.* § 164.504(f)(2)(ii).

[46] *See id.* §§ 164.504(f)(1)(ii), 164.504(a), 164.530(k)(1)(B).

[47] These programs are either Excepted Benefits or they do not provide or pay for the cost of Medical Care. Programs such as pre-employment physicals and annual testing of healthcare workers also are considered employer functions rather than Health Plan functions, and information held by an employer with respect to these and other employer activities is not subject to the Privacy Rule. Issues related to the limits on and separation of these employer functions, however, must be addressed in the context of Privacy Rule compliance efforts. *See* 42 U.S.C. § 300gg-91(a)(2) (2004); 45 C.F.R. § 160.103 (2004); Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462, 82,567 (Dec. 28, 2000) (to be codified at 45 C.F.R. pts. 160, 164).

[48] An exception is made for disclosures of protected health information by a covered entity as authorized by and to the extent necessary to comply with laws relating to worker's compensation or similar programs established by law that provide benefits for work-related injuries or illness without regard to fault. *See* 45 C.F.R. § 164.512(1) (2004).

[49] *See infra* notes 75-81 and accompanying text (discussion of the meaning and difference between insured and self-insured plans).

[50] *See* 45 C.F.R. § 160.103 (2004).

[51] *See id.* § 164.530(k)(1)(B) (defining summary health information and enrollment and disenrollment information).

[52] *Id.* § 164.530(g). Specifically, the Privacy Rule provides as follows:

> A covered entity may not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against: (1) Individuals. Any individual for the exercise by the individual of any right under, or for participation by the individual in any process established by this subpart, including the filing of a complaint under this section; (2) Individuals and others. Any individual or other person for: (i) Filing of a complaint with the Secretary under subpart C pf part 160 of this subchapter; (ii) Testifying, assisting or participating in an investigation, compliance review, proceeding, or hearing under Part C or Title XI; or (iii) Opposing any act or practice made unlawful by this subpart, provided the individual or person has a good faith belief that the practice opposed is unlawful, and the manner of opposition is reasonable and does not involve a disclosure of protected health information in violation of this subpart.

Id. § 164.530(g).

[53] *Id.* § 164.530(h). As a practical matter, however, the sponsor may be advised to do the following: (1) ensure its insurance agreements address HIPAA compliance issues; (2) confirm that an authorization has been obtained from any employee whose protected health information is disclosed by the insurance issuer or HMO to the sponsor; (3) educate its employees to recognize cases in which protected health information may be improperly disclosed to them and also to facilitate compliance with the statutory obligations to refrain from retaliation and/or requiring a waiver; and (4) adopt policies and procedures for dealing with both improper disclosures and proper disclosures made pursuant to authorizations, including policies and procedures designed to prevent the use or disclosure of any protected health information disclosed to the sponsor pursuant to an authorization, as well as policies and procedures to facilitate compliance with the statutory obligations to refrain from retaliation and requiring a waiver.

[54] *See generally* Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462, 82,627-28 (Dec. 28, 2000) (to be codified at 45 C.F.R. pts. 160, 164); Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. 53,182, 53,248 (Aug. 14, 2002) (to be codified at 45 C.F.R. pts. 160, 164). TPAs are service companies that provide one or more management and/or administrative services to a Health Plan, performing these services on

behalf of the plan but not assuming any of the insurance risk associated with the Medical Care. When TPA services are provided by an entity that is also an insurance issuer or HMO for other purposes, the arrangement typically is referred to as an "administrative services only" or ASO arrangement, but the relationship is essentially the same.

[55] *See* 45 C.F.R. §§ 164.502(b)-164.514(d) (2004). Under the Rule, these Business Associate Contracts must establish the permitted and required uses and disclosures of protected health information by the Business Associate, and provide generally that the Business Associate will: (i) not use or further disclose the information other than as permitted or required by the contract; (ii) use appropriate safeguards to prevent unauthorized use or disclosure of that information; (iii) report to the Health Plan any unauthorized use or disclosure of which the Business Associate becomes aware; (iv) ensure that any agents or subcontractors to which it provides the information agree to the same restrictions and conditions; (v) make available the information as necessary for the Health Plan to respond to the exercise by an individual of his or her rights under the Rule with respect to that information and comply with certain of those rights if directed by the Health Plan; (vi) make its books or records available to the DHHS Secretary; (vii) authorize termination of the contract if the Health Plan believes the Business Associate has violated a material term; and (viii) upon termination of the contract, return or destroy all the information if feasible and, if not feasible, extend the protections of the contract to that information and limit uses and disclosures to those that made the return or destruction infeasible. *Id.* § 164.504(e).

[56] *See id.* §§ 164.502(b)-164.514(d). When entering into a Business Associate Agreement with a TPA, a sponsor is contracting on behalf of the Health Plan, which is the Covered Entity. An interesting dichotomy is raised by this requirement. This is true because a sponsor that receives protected health information for the performance of administration functions for the plan and has complied with the Sponsor Requirements also has the option of contracting on behalf of itself as a sponsor with a third party to perform those administration functions on behalf of the sponsor (who is performing them on behalf of the plan) rather than contracting directly on behalf of the plan. The interesting issues raised are that if a sponsor contracts on behalf of the plan, it may then limit its technical receipt of protected health information. The Business Associate obligations imposed on the TPA are onerous and numerous. On the other hand, if the sponsor takes on the responsibility of performing all administration functions for the plan and subcontracts those out to the TPA, technically the sponsor is in receipt of substantial protected health information. As such, the obligations the Rule requires the sponsor to put on the TPA are much more general and less onerous. As a result, the advisable route for sponsors is to contract with the TPA on behalf of the plan, although this distinction in practice is often missed.

[57] *See* Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. at 53,248. Some TPAs have attempted to negotiate rights that go beyond those provided by the Rule, such as obtaining representations and warranties of compliance by the Health Plan or obtaining the right to use protected health information for research. Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. at 53,248. Some even attempt to wholly circumvent the Business Associate obligations by requiring the Health Plan to assume the responsibility for compliance by the TPA of those obligations. Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. at 53,248.

[58] The risk for a sponsor associated with transferring fiduciary responsibility under a self-insured plan to a third-party contractor and not having access to any individual level claims data is that the sponsor is the party financially responsible for paying the claims, yet would have no role in determining which claims will be paid nor access to data relating to large dollar claims.

[59] *See, e.g.,* Sentencing Reform Act, 18 U.S.C. § 3551 (2004).
[60] *Compare* Crosby v. Nat'l Foreign Trade Council, 530 U.S. 363, 388-91 (2000) (Scalia, A., concurring in the judgment) *with* Stephen Breyer, *On the Uses of Legislative History in Interpreting Statutes*, 65 S. CAL. L. REV. 845 (1992).
[61] *See, e.g.,* Sarbanes-Oxley Act of 2002, 15 U.S.C. § 7201 (2004); Press Release, U.S. Sec. and Exch. Comm'n, Summary of SEC Actions and SEC Related Provisions Pursuant to the Sarbanes-Oxley Act of 2002 (July 30, 2003), *available at* www.sec.gov/news/press/2003-89a.htm (last visited Apr. 5, 2004).
[62] *See supra* text accompanying note 58.
[63] *See* Kirk S. Jordan & Joseph E. Murphy, *Ethics and Compliance Programs: What the Government Really Wants*, Integrity Interactive, *at* www.integrity-interactive.com/compliance/mkt_expertise_pg6.htm (last visited Apr. 5, 2004) (a thoughtful discussion of the Sentencing Guidelines and a review of cases settled subsequent to adoption of those guidelines to show empirical evidence of specific measures governmental agencies expect in an organization's compliance program).
[64] Jordan & Murphy state that no reported cases exist interpreting what is meant by an "effective" program under the Sentencing Guidelines. *Id.* at 2.
[65] News Release, American Bar Association, ABA Adopts New Lawyer Ethics Rules, Urges Fairness in Military Commission Trials (Aug. 12, 2003), *available at* www.abanet.org/media/aug03/081203_1.html (last visited Apr. 5, 2004).
[66] *Id.*
[67] Nicholas Quinn Rosenkranz, *Federal Rules of Statutory Interpretation*, 115 HARV. L. REV. 2085 (2002).
[68] *See generally id.* at 2086.
[69] To a certain extent, Rosenkranz reports on the more germane and significant participants and theories of this debate in his article, from the new textualism championed by Justice Scalia and by Judge Easterbrook to the dynamic statutory interpretation theories of Professor William N. Eskridge. *Id.* The fabric of the discourse, however, is being woven even more richly than reported by Rosenkranz. *See* Harold P. Southerland, *Theory and Reality in Statutory Interpretation*, 15 ST. THOMAS L. REV. 1 (2002). Professor Southerland passionately and beautifully presents a humanistic philosophical critique of Justice Scalia's new textualism, which Southerland contends "ignores the inexactitude of language generally and American English in particular" as well as taking "no account of the failings and foibles of the human beings who people [the world.]" *Id.* at 12, 14. *See also* Joseph A. Grundfest & A. C. Pritchard, *Statutes With Multiple Personality Disorders: The Value of Ambiguity in Statutory Design and Interpretation,* 54 STAN. L. REV. 627 (2002). The latter article proffers the view that the adoption of any consistent rule of statutory interpretation is bound to fail because it would "seek to impose a degree of uniformity in interpretation that is inconsistent with the equilibrium relationship between the legislative and judicial branches." *Id.* at 636. Grundfest and Pritchard argue that legislators have a vested interest in ambiguity because it can credibly be argued to support opposing viewpoints and garner more widespread constituent support. They also argue that judges have a vested interest in ambiguity because it leaves them more room to exercise judicial discretion. *Id.* at 628-29. As if that argument alone is not enough, the authors perform a statistical analysis of appellate opinions relating to a specific statutory standard to determine which interest wins out. They conclude that the congressional ability to obscure prevails over the judiciary's ability to interpret at the appellate level. *Id.* at 634, 671.
[70] Rosenkranz notes that his article, which proposes that Congress adopt federal rules, questioned the "central, unquestioned premise" in the field of statutory interpretation "that the judiciary is the proper branch to design and implement tools of statutory interpretation." *See* Rosenkranz, *supra* note 67, at 2086.
[71] *Id.*
[72] *See* Grundfest & Pritchard, *supra* note 69, at 636-39 (arguing that Congress often favors ambiguity over clarity).

[73] *See* Rosenkranz, *supra* note 67 (Rosenkranz's treatment generally of the constitutional limitations on congressional authority to legislate interpretive rules and standards).
[74] *See, e.g.,* 42 U.S.C. § 1320d (2004).
[75] Most healthcare FSAs and EAPs qualify as small health plans under HIPAA and thus had until April 14, 2004, to comply with the Privacy Rule. 45 C.F.R. § 164.534(b)(2) (2004).
[76] *See infra* notes 93-96 and accompanying text (discussion of Catchall Category plans).
[77] Dept. of Health and Human Servs., *Questions and Answers: Is a flexible spending account or a cafeteria plan a covered entity?* (April 24, 2003) (addressing whether a flexible spending account or a cafeteria plan is a Covered Entity), *at* tinyurl.com/2tbuh (last visited Apr. 25, 2004) [hereinafter *Questions and Answers*].
[78] *See* 45 C.F.R. § 160.103 (2004).
[79] The Rule provides as follows:

> *Health insurance issuer* (as defined in section 2791(b)(2) of the PHS Act, 42 U.S.C. 300gg-91(b)(2) and used in the definition of health plan in this section) means 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.

Id. (emphasis added).
[80] The Rule provides as follows:

> *Health maintenance organization* (HMO) (as defined in section 2791(b)(3) of the PHS Act, 42 U.S.C. 300gg-91(b)(3) and used in the definition of health plan in this section) means a federally qualified HMO, an organization recognized as an HMO under State law, or a similar organization regulated for solvency under State law in the same manner and to the same extent as such an HMO.

Id. (emphasis added).
[81] *See* Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462, 82,645 (Dec. 28, 2000) (to be codified at 45 C.F.R. pts. 160, 164).
[82] *See* 45 C.F.R. § 160.103 (2004). If an FSA did not meet the definition of an ERISA plan, employers would be faced with the question whether it was captured by the Catchall Category of "other health plans." *See infra* notes 93-96 and accompanying text.
[83] Some industry participants have interpreted a wrap-around plan as requiring a hybrid entity structure, but in reality the structure does not seem to make much difference in compliance, particularly with the definition of Health Plans having the same sponsor as an organized healthcare arrangement.
[84] It is possible that a sponsor can avoid most of these compliance requirements by restructuring its arrangement with its TPA such that: (i) the TPA agrees to assume the Health Plan compliance responsibilities described in Part I.B on behalf of the FSA; and (ii) the TPA agrees to assume the ERISA fiduciary responsibility for final claims adjudication and the sponsor provides the TPA with the right to draw on accounts maintained by the sponsor for the purpose of claims payment. In this case, the TPA will manage the accounting for the funds in a way that protected health information is never disclosed to sponsor. The TPA simply reports in the aggregate to the sponsor the total amounts reimbursed to enrollees without allocating the total to the participating individuals. Transferring the accounting responsibilities to the TPA could involve some modest additional financial risk for the sponsor in that the sponsor would not be able to audit the TPA's claims payment or accounting.

[85] *See* Application of HIPAA Group Market Portability Rules to Health Flexible Spending Arrangements, 62 Fed. Reg. 67,688 (Dec. 29, 1997) (to be codified at 29 C.F.R. pt. 2590, 45 C.F.R. subtit. A, pts. 144, 146, 26 C.F.R. pt. 54).

[86] *Questions and Answers, supra* note 77 (citations omitted). Some discussion on industry listserves has tried to characterize the DHHS answer as not being definitive because it essentially states that an FSA is a Health Plan that is an ERISA plan and begs the questions whether an FSA is an ERISA plan. It is difficult to imagine, however, a convincing argument that an FSA is not an ERISA plan.

[87] *See* Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462, 82,577 (Dec. 28, 2000) (to be codified at 45 C.F.R. pts. 160, 164).

[88] The one Excepted Benefit that is not consistent with this principle is the on-site medical clinic.

[89] *See* 45 C.F.R. 160.103 (2004).

[90] Dep't of Labor Employee Benefits Security Admin. (formerly PWBA), Opinion Letter 88-04A (Mar. 11, 1988), available at 1988 WL 360954.

[91] *Id*.

[92] Some entities have argued that an EAP provider may meet the Catchall Category definition as a plan or program that pays for the cost of Medical Care because the EAP provider bears some financial risk for providing the care and pays the counselors or care providers directly. This argument appears to be misguided because the Catchall Category is defined as an individual plan or program that provides or pays for certain benefits. An EAP provider has no contractual privity with the beneficiaries of its services, thus it is not an individual or group plan or program—it simply administers a plan or program provided by the employer, and that plan or program does have contractual privity with, and obligations to, the beneficiaries.

[93] *Compare* 45 C.F.R. § 160.103 *with* ERISA § 3(1) , 29 U.S.C. § 1002(1) (2004).

[94] *See* Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462, 82,577 (Dec. 28, 2000) (to be codified at 45 C.F.R. pts. 160, 164).

[95] *Id*. at 82,576.

[96] *Id*. at 82,578.

[97] 45 C.F.R. § 164.502(a)(1)(iv) (2004).

[98] *See generally id.* § 164.508 (general requirements for, and core elements of, a valid authorization under the Rule). The instances in which a Covered Entity is allowed to condition the provision of services or benefits on the provision of an authorization include cases in which the treatment or benefit is for the sole purpose of creating protected health information for disclosure to a third party, such as pre-employment physicals and employer drug testing. *Id.* § 164.508(b)(4)(iii). The other two exceptions to this general prohibition relate to research-related treatment and health plan initial enrollment and eligibility determinations. *Id*. § 164.508(b)(4)(i)-(ii).

[99] *See generally id.* § 164.508(b)(4).

[100] For a list of these requirements, *see supra* text accompanying notes 38-46.

[101] A Health Plan is required under the Rule to disclose in its notice of privacy practices provided to enrollees. *See* 45 C.F.R. §§ 164.502(b)-164.514(d), 164.520(b)(1)(iii)(C) (2004).

[102] *Id*. § 164.504(f)(2)(ii)(C).

[103] *See* 42 U.S.C. § 300gg-91(a)(2) (2004).

[104] *See id*. § 300gg-91(a)(2).

[105] *See Questions and Answers, supra* note 77.

[106] Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462, 82,577 (Dec. 28, 2000) (to be codified at 45 C.F.R. pts. 160, 164).

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

[108] *Id*. at 53,182.

[109] *Id*.
[110] Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. at 82,463.
[111] *Id*. at 82,464.
[112] *Id*. at 82,471.
[113] *Id*.
[114] *Id*. at 82,472.
[115] *Id*.
[116] *See* 45 C.F.R. § 164.103 (2004) (defining "plan sponsor").
[117] *See generally id*. § 164.508
[118] *See generally id*.
[119] *Id*. § 164.504(f)(2)(ii)(C).
[120] "Except as otherwise permitted or required . . . a covered entity may not use or disclose protected health information without an authorization that is valid under this section." *Id*. § 164.508(a)(1).