



March 3, 2005

Sam Francis, Esq.  
President  
Texas Professional Benefit Administrators Association  
P.O. Box 380236  
Duncanville, TX 75138-0236

Dear Mr. Francis:

The purpose of this letter is to analyze the issue of whether the issuer of a group health insurance policy is permitted under the Standards for Privacy of Individually Identifiable Health Information, 45 C.F.R. Parts 160 and 164 (the "Privacy Standards"), enacted pursuant to the Health Insurance Portability and Accountability Act of 1996, as amended, 29 U.S.C. §§ 1181, *et seq.* ("HIPAA"), and under the Employee Retirement Income Security Act of 1974, as amended, 29 U.S.C. §§ 1001, *et seq.* ("ERISA"), to provide an individual's protected and individually identifiable health information (as defined in the Privacy Standards at 45 C.F.R. § 164.501, "Protected Health Information" or "PHI") to the employer that sponsors the employee group health plan to which the policy relates.

As explained in the remainder of this letter, it is clear that:

1. The issuer of a group health insurance policy and a health maintenance organization ("HMO") are permitted, under the Privacy Standards and under ERISA, to provide an individual's Protected Health Information to the employer that sponsors the employee group health plan to which the policy relates, as permitted by the employee group health plan and federal law;
2. The issuer of a group health insurance policy and an HMO are permitted, under the Privacy Standards and under ERISA, to provide an individual's Protected Health Information to the employer, either as the Administrator (as defined below) of the plan to which the policy relates, or as another fiduciary of the plan, to the extent requested by the employer;
3. The issuer of a group health insurance policy and an HMO are permitted, under the Privacy Standards and under ERISA, to provide an individual's Protected Health Information to the employee group health plan to which the policy relates, to the extent requested by such plan, as the relationship between the issuer or the HMO, on the one hand, and the plan, on the other hand, is considered to be that of an "Organized Health Care Arrangement" or "OHCA" with respect to PHI created or received by such health insurance issuer or HMO that relates to individuals who are or who have been participants or beneficiaries in such group health plan;
4. While the Privacy Standards state that the issuer of a group health insurance policy or an HMO is permitted to provide an individual's Protected Health Information, as set forth in paragraphs 1 through 3 above (45 C.F.R. §§ 164.501, 164.504(f)(3) and 164.506), the Privacy Standards do not state that the issuer or HMO is permitted to refuse to provide such PHI;

*Attorneys at Law*



The Forgie-Provins House, 311 Allison Avenue, Washington, PA 15301

Phone: (724) 222-2521 ☎ Fax: (724) 222-2699 ☎ Email: [thefirm@rizzagroup.com](mailto:thefirm@rizzagroup.com) ☎ [www.rizzagroup.com](http://www.rizzagroup.com)

Sam Francis, Esq.  
March 3, 2005  
Page 2 of 8

5. Providing such PHI to the employer or plan, as set forth in paragraphs 1 through 3 above, would not violate either the Privacy Standards or ERISA;
6. A refusal to provide such PHI to the employer would cause an employer to be in violation of ERISA; and
7. No duty or authority exists, on the part of the health insurance issuer or the HMO, to determine if the PHI requested is the minimum necessary PHI needed to accomplish the intended purpose or to question the employer's compliance with the Privacy Standards.

#### The Privacy Standards in General.

The Privacy Standards are designed to prevent PHI from being used or disclosed by Covered Entities (which, under the Privacy Standards, essentially are health plans, health care providers who transmit health information in electronic form and health care clearinghouses) without the individual's express authorization, except as explicitly permitted or required in certain limited circumstances. The Privacy Standards restrict how a Covered Entity may use and disclose PHI – including when a use or disclosure is required or permitted – and the conditions relating to the use or disclosure. Covered Entities' uses or disclosures of, or requests for, PHI must consist of only the minimum amount necessary to accomplish the intended purpose of the use, disclosure, or request.

#### The Employer as Plan Sponsor.

ERISA defines "Plan Sponsor" as the "employer in the case of an employee benefit plan established or maintained by a single employer..." (29 U.S.C. § 1002(16)(B)). Accordingly, in the context of a single-employer employee group health plan, whether fully insured or self-funded, the Plan Sponsor is the employer. When the employer is acting as the Plan Sponsor, it is not a fiduciary of the plan; rather, it is acting in a settlor capacity (that is, similar to a person establishing a trust) and has four responsibilities: establishing, amending, terminating and funding the plan.

Preliminarily, a group health plan, or a health insurance issuer or HMO with respect to the group health plan, may disclose Summary Health Information (as defined below) to the Plan Sponsor, if the Plan Sponsor requests it for the purpose of (a) obtaining premium bids from health plans for providing health insurance coverage under the group health plan, or (b) modifying, amending or terminating the group health plan. 45 C.F.R. § 164.504(f)(ii). Plan documents need not be amended to enable disclosure of Summary Health Information in these situations. Further, without the need to amend plan documents, the Privacy Standards indicate that a group health plan, or a health insurance issuer or HMO with respect to the group health plan, may disclose to the Plan Sponsor information on whether an individual is participating in the plan, or is enrolled in or has disenrolled from a health insurance issuer or HMO offered by the plan. 45 C.F.R. § 164.504(f)(iii).

"Summary Health Information" is defined in the Privacy Standards as information that may be individually identifiable health information, and (1) that summarizes the claims history, claims expenses, or types of claims experienced by individuals for whom a Plan Sponsor has provided benefits under a group health plan; and (2) from which the following information has been deleted, except that the geographic information described in (B) below need only be aggregated to the level of a five digit zip code.

Sam Francis, Esq.  
March 3, 2005  
Page 3 of 8

The information that must be deleted includes the following identifiers of the individual or of relatives, employers, or household members of the individual:

- (A) Names;
- (B) All geographic subdivisions smaller than a state, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census:
  - (1) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and
  - (2) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000;
- (C) All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death, and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
- (D) Telephone numbers;
- (E) Fax numbers;
- (F) Electronic mail addresses;
- (G) Social security addresses;
- (H) Medical record numbers;
- (I) Health plan beneficiary numbers;
- (J) Account numbers;
- (K) Certificate/license numbers;
- (L) Vehicle identifiers and serial numbers, including license plate numbers;
- (M) Device identifiers and serial numbers;
- (N) Web Universal Resource Locators (URLs);
- (O) Internet Protocol (IP) address numbers;
- (P) Biometric identifiers, including finger and voice prints;
- (Q) Full face photographic images and any comparable images; and
- (R) Any other unique identifying number, characteristic, or code, except for a code or other means of record identification that is not derived from or related to information about the individual and is not otherwise capable of being translated so as to identify the individual, where the Covered Entity does not use or disclose the code or other means of record identification for any other purpose and does not disclose the mechanism for re-identification. 45 C.F.R. §§ 164.504(a) and 164.514(b) and (c).

Once all of the above information is deleted, it is obvious that the remaining information will be of little or no value. As a result, the employer will need more than Summary Health Information to perform its duties as Plan Sponsor, such as obtaining quotes for group health insurance from another insurer or excess loss insurance should the employer consider partial self-funding of its plan. Rather, it will require Protected Health Information. For example, the employer as Plan Sponsor needs detailed claims information beyond a one-line tally of total claims and total dollar amount paid (which is essentially what is included in Summary Health Information) to negotiate premiums with a current group health insurer or to shop for quotes from other group health insurers and excess loss insurers. Without this detailed claims experience, a Plan Sponsor may not get a quote from another insurer at all, or the quote may be exceedingly high because of the insurer's fear about hidden health risks. This PHI is necessary to identify

Sam Francis, Esq.  
March 3, 2005  
Page 4 of 8

large claimants or those with high risk. In some cases, this PHI may show that the claimant is no longer covered by the plan or that the risk is not as bad as it first appears, thereby resulting in savings to the plan.

Further, this PHI is needed by the Plan Sponsor to oversee the costs of their health plan and to correct situations such as where charges for an on-the-job injury erroneously are applied to the health plan rather than a separate workers' compensation plan. It also is essential to show the Plan Sponsor how their health care dollars are being spent and how they can be spent more efficiently. Without this type of data analysis, the Plan Sponsor is unable to determine where the dollars are being spent and what design changes are appropriate.

For these reasons, receipt of only Summary Health Information, as well as enrollment and disenrollment information, is not a prudent method for dealing with the Privacy Standards for the employer acting as Plan Sponsor.

It is clear that the Privacy Standards contemplate this determination by a Plan Sponsor, as they provide a mechanism for getting PHI to the Plan Sponsor, by stating that a group health plan may: (i) disclose PHI to a Plan Sponsor to carry out Plan Administration functions (which are administration functions performed by the Plan Sponsor of a group health plan on behalf of that plan, excluding functions performed by the Plan Sponsor in connection with any other benefit or benefit plan of the Plan Sponsor) that the Plan Sponsor performs consistent with certain restrictions<sup>1</sup> on the use and disclosure of such information that must be contained in the plan documents; (ii) not permit a health insurance issuer or HMO with respect to the group health plan to disclose PHI to the Plan Sponsor except as permitted by the Privacy Standards; (iii) not disclose and not permit a health insurance issuer or HMO to disclose PHI to a Plan Sponsor as otherwise permitted by the Privacy Standards unless the plan's privacy notice contains a statement that the plan, or a health insurance issuer or HMO with respect to the plan, may disclose PHI to the Plan Sponsor; and (iv) not disclose PHI to the Plan Sponsor for the purpose of employment-related actions or decisions or in connection with any other benefit or employee benefit plan of the Plan Sponsor. 45 C.F.R. § 164.504(f)(3).

#### The Employer as the Plan's Administrator.

ERISA defines "Administrator" as "(i) the person specifically so designated by the terms of the instrument under which the plan is operated; [or] (ii) if an [A]dministrator is not so designated, the [P]lan [S]ponsor...." (29 U.S.C. § 1002(16)(A)). The plan's Administrator is responsible for all of the operations and administration of the plan, unless the plan documents allocate certain responsibilities to other fiduciaries. In a single-employer, fully insured arrangement, the employer always will be the Plan Sponsor and it also may act as the plan's Administrator. In some instances, the insurer acts as the plan's Administrator. More often, the employer is the plan's Administrator. This information can be found in the plan documents (such as the summary plan description or benefit booklet) and contract with the insurer. It is common to find that the insurer will take responsibility for decisions as to whether or not claims are payable under the plan, but leaves all other decisions, including those relating to eligibility, to the employer. However, even if the insurer acts as the plan's Administrator, the employer still must act as

<sup>1</sup> These restrictions are the completion of designated amendments to plan documents and establishment of certain procedures (to provide for separation of the plan from the Plan Sponsor, to comply with individuals' rights relating to PHI, and to address destruction and maintenance of PHI). 45 C.F.R. § 164.504(f)(2). In addition, the employer will be required to certify to the plan's Administrator in writing that, as Plan Sponsor, it has complied with these provisions and that the plan documents have been appropriately amended. Of course, if the employer serves as both Plan Sponsor and plan's Administrator, it will be providing a certification to itself. 45 C.F.R. § 164.504(f)(2)(ii). Essentially, the employer will be required to separate its functions as a fiduciary of the plan from those relating to its position as Plan Sponsor, as well as those relating to it as an employer. This can be as simple as delegating these duties to different individuals or different departments within the employer's organization and safeguarding the PHI each of those individuals or departments can access.

Sam Francis, Esq.  
March 3, 2005  
Page 5 of 8

a fiduciary with respect to the plan. Under ERISA, something as simple as the employer helping an employee enroll in the plan is considered to be a fiduciary action. In the context of a fully insured plan, the employer is required to do that, plus many other things, such as fulfilling the requirements of the Consolidated Omnibus Budget Reconciliation Act of 1985, as amended ("COBRA"), determining eligibility of plan participants, and providing assistance to participants whose claims are denied by the carrier, all of which constitute fiduciary functions and make the employer a fiduciary of the plan.

Under ERISA, the plan's Administrator and other fiduciaries are required to discharge their duties with respect to a plan solely in the interest of the participants and beneficiaries and: (A) for the exclusive purpose of providing benefits to participants and their beneficiaries and defraying reasonable expenses of administering the plan; (B) with the care, skill, prudence, and diligence under the circumstances then prevailing that a prudent man acting in a like capacity and familiar with such matters would use in the conduct of an enterprise of a like character and with like aims; (C) by diversifying the investments of the plan so as to minimize the risk of large losses, unless under the circumstances it is clearly prudent not to do so; and (D) in accordance with the documents and instruments governing the plan insofar as such documents and instruments are consistent with ERISA. 29 U.S.C. § 1104. Clearly, it is impossible for an employer to administer a plan in a manner that will satisfy this requirement without full access to PHI.

Technically, under the Privacy Standards, the plan's Administrator is not a Covered Entity; rather, the Covered Entity is the plan itself. However, for all practical purposes, the plan is nothing more than its plan document and summary plan description and perhaps a bank account. This is true even in the context of a fully insured plan. While the employee group health plan is a legal entity separate and apart from the employer, the insurer and the HMO, in actuality, it consists of only the benefit booklet or summary plan description that is distributed to the plan's participants and some books and records. Its actions are taken by the plan's Administrator and any other fiduciaries, which essentially makes the plan's Administrator and any other fiduciaries Covered Entities.

Under the Privacy Standards, if the employer is the plan's Administrator or a fiduciary of the plan, the employer is entitled to full access to PHI and is permitted to use PHI for TPO activities.<sup>2</sup> 45 C.F.R.

<sup>2</sup> "TPO" refers to treatment, payment and health care operations.

- "Treatment" means the provision, coordination or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient from one health care provider to another. "Treatment" does not relate to activities of health plans.
- "Payment" means activities undertaken by (a) the plan to obtain premiums or determine or fulfill its responsibility for coverage and the provision of plan benefits or (b) a health care provider or plan to obtain or provide reimbursement for the provision of health care. Additionally, the activities must relate to the individual to whom health care is provided. The Privacy Standards set forth various activities that could be considered "payment": eligibility determinations; coverage determinations; coordination of benefits; determination of cost-sharing amounts (such as plan maximums and co-payments); adjudication of health benefit claims, appeals and benefit disputes; subrogation and reimbursement of health benefit claims; risk-adjusting amounts due based on enrollee health status and demographic characteristics; billing and collection activities; claims management and related health care data processing, including auditing payments, investigating and resolving payment disputes and responding to participant inquiries regarding payments; obtaining payment under a contract for reinsurance, stop-loss insurance or excess loss insurance; medical necessity reviews, or reviews of coverage under a health plan, appropriateness of care or justification of charges; utilization review, including precertification, preauthorization, concurrent review and retrospective review; and disclosure of certain information to consumer reporting agencies related to the collection of premiums or reimbursement. "Payment" encompasses preparation of explanation of benefits (EOB) statements.
- "Health care operations" means any of the following activities of a Covered Entity that maintains PHI: quality assessment and improvement activities (including outcomes evaluation and development of clinical guidelines, except if the purpose of studies resulting from such activities is to gain generalized knowledge); population-based activities (which are activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, and contacting providers and patients with information about treatment alternatives and related functions that do not include treatment); reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance and plan performance; underwriting and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits, as well as ceding, securing or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess loss insurance); conducting or arranging for medical review, legal services and auditing functions, including fraud and abuse detections and compliance programs; business planning

Sam Francis, Esq.  
March 3, 2005  
Page 6 of 8

§ 164.506. A review of the definition of TPO activities shows that this is an extremely broad range of activities for which the employer may access PHI. The plan's Administrator or other fiduciary must have appropriate procedures in place to protect the PHI, addressing verification of identity and authority in connection with disclosures of PHI, compliance with the "minimum necessary" requirements of the Privacy Standards, firewalls and employee access in connection with the Privacy Standards, non-compliance with the Privacy Standards, destruction and maintenance of PHI, and compliance with individuals' rights regarding PHI. 45 C.F.R. § 164.530(i).

"Covered Entities" in the Context of a Fully Insured Employee Health Benefit Plan: Relationship between the Insurer or HMO and the Employer.

In the situation where an employer has purchased a group health insurance policy for the benefit of its employees from a health insurance issuer or HMO and provides the benefits pursuant to an employee welfare benefit plan established under, and governed by, ERISA, there are two Covered Entities – the group health plan established by the employer and the insurance company or HMO. Under the Privacy Standards, the relationship between the group health plan and the insurance company or HMO is considered to be that of an "Organized Health Care Arrangement" or "OHCA" with respect to PHI created or received by such health insurance issuer or HMO that relates to individuals who are or who have been participants or beneficiaries in such group health plan. 45 C.F.R. § 164.501.

Disclosure of PHI by the Insurer or HMO.

*To the employer as the Plan Sponsor.* As set forth above, when the employer is acting as the Plan Sponsor, PHI may be provided as previously discussed on page 4. It is important to note here that the entity making the decisions as to whether or not the employer, as the Plan Sponsor, is provided with PHI is the group health plan, not the health insurance issuer or HMO.

*To the employer's plan and to the employer as the plan's Administrator.* Further, under the Privacy Standards, the plan, as a Covered Entity (and by virtue of its full authority for plan operations, the plan's Administrator, which may be the employer), has full access to all information relating to the Plan, including PHI. The health insurance issuer or HMO is a fiduciary only to the extent of its discretionary decisions made regarding claims and appeals. It does not have the fiduciary authority to determine what information may be provided to, or withheld from, the employer, as the plan's Administrator, and has only such minimum access to PHI as is necessary to perform its duties under the group health insurance policy. On December 3, 2002, the U.S. Department of Health and Human Services ("HHS") issued Guidance (the "HHS Guidance") that states that Covered Entities are required to apply the minimum necessary standard to their own requests for Protected Health Information. The HHS Guidance may be found at: <http://www.hhs.gov/ocr/hipaa/guidelines/guidanceallsections.pdf>. One Covered Entity may reasonably rely on another Covered Entity's request as the minimum necessary and, therefore, does not need to engage in a separate minimum necessary determination. See 45 C.F.R. § 164.514(d)(3)(iii) and HHS Guidance at p. 9. Accordingly, neither the group health plan, on the one hand, nor the health insurance issuer or HMO, on the other hand, is required to determine if the PHI requested by the other is

---

and development; business management and general administration (which include, but are not limited to: (1) management activities relating to implementation of and compliance with the requirements of the Privacy Standards; (2) customer service, including the provision of data analyses for policy holders, Plan Sponsors or other customers, provided that PHI is not disclosed to such policy holder, Plan Sponsor or customer; (3) resolution of internal grievances; (4) the sale, transfer, merger or consolidation of all or part of the Covered Entity with another Covered Entity, or an entity that following such activity will become a Covered Entity, and due diligence related to such activity; and (5) consistent with the applicable requirements of the Privacy Standards, creating de-identified health information or a Limited Data Set, and fundraising for the benefit of the Covered Entity); and disease management.

Sam Francis, Esq.  
March 3, 2005  
Page 7 of 8

the minimum necessary needed to accomplish the intended purpose. Rather, the Privacy Standards place the responsibility for that determination on the Covered Entity making the request. As a result, the health insurance issuer or HMO is permitted to disclose to the group health plan all PHI that the plan requests. The permissive nature of the cited regulations allows the health insurance issuer or HMO to disclose requested PHI to the plan without violating HIPAA. Refusal on the part of the health insurance issuer or HMO to disclose PHI to the plan's Administrator as allowed by the Privacy Standards would place the plan's Administrator in the unenviable position where, as a result of insufficient information, it cannot fulfill its ERISA fiduciary duties, thereby resulting in a separate violation of ERISA. See 29 U.S.C. § 1109 as well as the discussion set forth below.

*To the employer's plan as a member of an OHCA.* The Privacy Standards expressly state that a Covered Entity that participates in an Organized Health Care Arrangement may disclose PHI about an individual to another Covered Entity that participates in the OHCA for any health care operations activities of the OHCA. 45 C.F.R. § 164.506(c)(5). The definition of "health care operations" can be found in Footnote 2. The HHS Guidance reiterates that where a group health plan purchases insurance from a health insurance issuer or HMO, the relationship between the group health plan and the health insurance issuer or HMO is defined by the Privacy Standards as an OHCA, with respect to the individuals they jointly serve or have served, and these Covered Entities are permitted to share Protected Health Information that relates to the joint health care activities of the OHCA. See HHS Guidance at p. 19. The HHS Guidance further states that no business associate contract is needed between the parties, and each such entity is independently required to observe its obligations under the Privacy Standards with respect to PHI. See HHS Guidance at pp. 17-18. The obligation to comply with the Privacy Standards rests with each Covered Entity in the OHCA, and neither Covered Entity has the duty, or the authority, to police the other's compliance.

Once again, it is emphasized that a refusal to provide PHI as permitted by the Privacy Standards would place an employer acting as a plan's Administrator in the unenviable position in which, as a result of insufficient information, it cannot fulfill its ERISA fiduciary duties, thereby resulting in the plan Administrator's violation of ERISA.

#### In Summary.

Based upon the foregoing, it is clear that (a) the issuer of a group health insurance policy and an HMO are permitted, under the Privacy Standards and under ERISA, to provide an individual's Protected Health Information (i) to the employer that sponsors the employee group health plan to which the policy relates, as permitted by the employee group health plan and federal law; (ii) to the employer, either as the Administrator of the plan to which the policy relates, or as another fiduciary of the plan, to the extent requested by the employer; (iii) to the employee group health plan to which the policy relates, to the extent requested by such plan, as the relationship between the issuer or the HMO, on the one hand, and the plan, on the other hand, are considered to be that of an Organized Health Care Arrangement with respect to PHI created or received by such health insurance issuer or HMO that relates to individuals who are or who have been participants or beneficiaries in such group health plan; (b) while the Privacy Standards state that the issuer of a group health insurance policy or an HMO is permitted to provide an individual's Protected Health Information, as set forth in (a) above, the Privacy Standards do not state that the issuer or HMO is permitted to refuse to provide such Protected Health Information; (c) providing such PHI to the employer or plan, as set forth in (a) above, would not violate either the Privacy Standards or ERISA; (d) a refusal to provide such PHI to the employer would cause an employer to be in violation of ERISA; and (e) no duty or authority exists, on the part of the health insurance issuer or the HMO, to

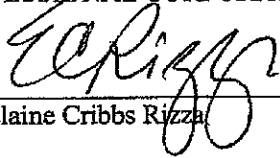
Sam Francis, Esq.  
March 3, 2005  
Page 8 of 8

determine if the PHI requested is the minimum necessary PHI needed to accomplish the intended purpose or to question the employer's compliance with the Privacy Standards.

Very truly yours,

THE RIZZA GROUP  
PROFESSIONAL CORPORATION

By:

  
\_\_\_\_\_  
Elaine Cribbs Rizza