

VIA ELECTRONIC DELIVERY AND MAIL

April 26, 2002

U.S. Department of Health and Human Services
Office for Civil Rights
Attention: Privacy 2
Hubert H. Humphrey Building
Room 425A
200 Independence Avenue, SW
Washington, DC 20201
<http://www.hhs.gov/ocr/hipaa>

Dear Sir or Madam:

These comments are filed by the National Coordinating Committee for Multiemployer Plans (NCCMP) in response to the request for public comments on the proposed modification of certain standards in the Final Rule entitled "Standards for Privacy of Individually Identifiable Health Information" (the "Privacy Rule"). These proposed modifications (contained in the Notice of Proposed Rulemaking or NPRM) were published in the Federal Register of March 27, 2001 (67 Fed. Reg. 14776). The Privacy Rule implements the privacy requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

The NCCMP is the only national organization devoted exclusively to protecting the interests of the approximately ten million workers, retirees, and their families who rely on multiemployer plans for retirement, health and other benefits. Our purpose is to assure an environment in which multiemployer plans can continue their vital role in providing benefits to working men and women. The NCCMP is a nonprofit organization, with members, plans and plan sponsors in every major segment of the multiemployer plan universe, including in the building and construction, retail food and service, and entertainment industries.

In general, the NCCMP supports the provisions of the Privacy Rule because we share the belief that privacy is a fundamental right. Americans' concern about the privacy of their health information is serious and deep. Particularly as the use of interconnected electronic information systems increase as a result of both marketplace pressures and external legal influences, it is critically important that personal medical records be protected.

We also share Congress' concern that this type of confidential information not be accessible to employers for employment-related purposes. At the same time, as sponsors

of multiemployer employee benefit plans providing health and other benefits, we need reasonable access to personal medical information in order to carry out our plan administration functions.

We commend the Department for its attempt to strike a balance between these two competing interests and generally support the special provisions in the Privacy Rule relating to group health plans and business associates. In particular, we are particularly grateful to the Department for including in its proposed modifications to the Privacy Rule a transition rule for the negotiation of business associate contracts and the model business associate contract language. Both provisions represent a positive step from the Department to make the Privacy Rule more workable and make compliance easier for covered entities.

However, there are still a number of issues that are of concern to multiemployer plans. In response to your request that comments should address only those sections of the Privacy Rule for which modifications are being proposed or comments requested through the NPRM, our comments will focus on just three areas: (1) the need for further clarification that enrollment and eligibility data (but not claims information) can be maintained in a database accessible by employers and other plan sponsors without need for adopting the special group health plan rules, (2) the suggestion that a new category of de-identified information might be established for benefit appeals, and (3) the desirability for the Department to promulgate a model authorization form.

1. Eligibility and Enrollment Databases

Background:

Multiemployer plans often have an eligibility and enrollment database that is shared between a multiemployer health plan and pension or disability plan. On some occasions, the union may also share the same eligibility database. The database is used to maintain common participant and beneficiary eligibility information, including the following:

- Name
- Address
- SSN or other member ID
- Name of dependent(s)

Similarly, a corporation or local or state government may have a human resources information system that maintains employee data and contains the above-mentioned items.

Multiemployer plans generally provide health benefits either through an insured arrangement, health maintenance organization, or through self-insurance. If the benefits are self-insured, they might be administered by the plan itself or administered by a Third

Party Administrator (TPA). Regardless of the health benefit delivery arrangement, a multiemployer plan itself might maintain its enrollment database. For example, a multiemployer plan may be fully insured, but maintain a database containing enrollment and eligibility information that is transmitted to the insurer. In this manner, the functions performed by the multiemployer plan are similar to that of a corporate plan sponsor.

The database would be used to determine eligibility for coverage under a benefit plan, verify addresses, and provide enrollment lists to an insurance company, HMO or TPA for claims or premium payment purposes. In addition, multiemployer plans have a fiduciary obligation to audit contributing employers to assure that the contributions made on behalf of individuals are accurate. The combined database is sometimes used to assist the plans' auditors as they attempt to determine whether the employer has properly reported individual eligibility for benefits.

Currently, the Federal agencies that administer the Employee Retirement Income Security Act of 1974 (ERISA) assume that the information contained in health plan enrollment and eligibility databases is available for other benefits and benefit plans. For example, the Pension Benefit Guaranty Corporation requires that pension plan sponsors looking for missing participants in connection with a pension plan termination conduct a "diligent search" to find those participants. Generally that search will include contacting companion health plans to ask for addresses for these individuals.

Although the database is shared by the employee benefit plans for the purposes of identifying individuals in the plan and verifying addresses, in a multiemployer plan context, it generally has no relation to the process of providing health benefits. For fully insured arrangements, the database is used to provide enrollment information to the insurance company or HMO. For self-insured arrangements using a TPA, the database is used to provide enrollment information to the TPA. If the plan is self-administered, firewalls and other protections assure that any systems used in the health claims operation cannot be accessed by individuals that do not have a need for that information. In addition, if a multiemployer group health plan retains an insurer or TPA to administer benefits, the plan has no access to the health claims information.

Relevant Sections of the Privacy Rule:

Section 164.501 of the Privacy Rule states that "protected health information" (PHI) means "individually identifiable health information" that is transmitted or maintained in electronic, written or oral media.

"Individually identifiable health information" is defined in Section 160.103 of the Privacy Rule as follows:

Individually identifiable health information is information that is a subset of health information, including demographic information collected from an individual, and:

- (1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
- (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and
- (3) That identifies the individual; or
- (4) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

NPRM Background:

In the preamble to the NPRM published on March 27, 2002, in its discussion of “hybrid entities,” the Department stated that it had received comments indicating that covered entities were concerned that they would be forced to treat the employment records of their employees as PHI. 67 Fed. Reg. at 14804.

Therefore, the NPRM proposes to clarify that PHI does not include employment records held by a covered entity, such as a physician’s office, hospital, or insurance company. But in the preamble to the NPRM, the Department also states that:

It is important to note that the exception from the definition of “protected health information” for employment records only applies to individually identifiable health information in those records that are held by a covered entity in its role as employer. The exception does not apply to individually identifiable health information held by a covered entity when carrying out its health plan or health care provider functions. Such information would be protected health information. Id.

To respond to that concern, Section 164.501 of the Privacy Rule is proposed to be modified as follows:

Protected health information means ***

(2) Protected health information excludes individually identifiable health information in:

- (i) Education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g;
- (ii) Records described at 20 U.S.C. 1232g(a)(4)(B)(iv); and
- (iii) Employment records held by a covered entity in its role as an employer.

67 Fed. Reg. 14804 (March 27, 2002).

The Department is soliciting comments from the public regarding what other issues exist with respect to whether “employment records” constitute PHI and must be protected under the privacy rule.

The issue of enrollment information is also briefly addressed in the preamble to the Privacy Rule. The Department states:

We note that a plan sponsor may perform enrollment functions on behalf of its employees without meeting the conditions above [the notice requirements of section 520 and the administrative requirements of section 530] and without using the standard transactions described in the Transactions Rule.

65 Fed. Reg. 82509 (December 28, 2000).

The preamble to the Privacy Rule contained the following somewhat cryptic language in its discussion of the new group health plan rules contained in Section 164.504(f):

... enrollment functions performed by the plan sponsor on behalf of its employees are not considered plan administration functions.

65 Fed. Reg. at 82508.

Also in the preamble, the Department indicated that disclosure of enrollment and disenrollment information to the plan sponsor without amending the plan or meeting the other requirements of Section 164.504(f) of the Rule was permissible. 65 Fed. Reg. at 82509 (Dec. 28, 2000).

In the NPRM, the Department proposes to add an explicit exception to Section 164.504(f)(1)(iii) to clarify that group health plans, health insurance issuers and HMOs may disclose enrollment and disenrollment information to a plan sponsor without meeting the plan document and other related requirements.

Discussion:

Prior to the issuance of the NPRM, we had a number of questions regarding the extent to which certain enrollment and eligibility information was PHI and the ability of multiemployer plans with centralized databases containing this information to continue to allow access to the information by other benefit plans of the plan sponsor. For instance, we were considering these questions:

- May information regarding name, address, and dependent information that is held in a database maintained by a health plan be shared with individuals that

are outside the health plan for purposes that are not related to treatment, payment or health care operations?

- For example, may a name and address list maintained by a health plan be shared with a companion pension plan?
- May a health plan provide a name and address list to a trustee of the fund (i.e., the plan sponsor)?
- May the health and pension funds access the same database for enrollment information?
- If a multiemployer plan is fully insured, and maintains no claims information, what obligations does the plan have with respect to protecting the name, address, and dependent information associated with its participants and beneficiaries?

The NPRM clarified the intent of the Department regarding enrollment information, but did not explain what enrollment information was. Based on the language of the Privacy Rule quoted above, some have argued that the Department may be considering only the simple statement of whether or not an individual is enrolled in the plan at the time of the disclosure to be enrollment information. But we believe that this is too narrow a reading of the Department's intent. Enrollment information commonly includes the type of information multiemployer plans have in their databases: names, addresses, social security numbers, the identity of the local union to which the employee belongs, the name of employer who is contributing on behalf of the employee and dependent information.

This type of information contained in the eligibility and enrollment database maintained by a multiemployer plan is similar to the employment information that an employer maintains. However, because the multiemployer health plan is not generally the employer of the participants in the plan, this information arguably remains protected health information, even under the NPRM, because it is held and used by the plan in connection with its covered functions, not as an employer.

We understand that a main focus of the privacy rule is preventing sharing of information obtained through a health benefit plan with groups that intend to use the information for purposes unrelated to the benefit plan, such as a prescription drug marketing campaign. However, employment records, eligibility information, enrollment information and premium payment information is not collected as part of an individual's health information record. Instead, it is collected by an employer or other plan sponsor, including a multiemployer plan's board of trustees, for the purpose of arranging for health benefit coverage. While we respect the principle of limiting this information, it should be freely available to employers and plan sponsors who collect it, as long as the information is not linked to claims data.

Recommendation:

The Department should adopt a clarifying amendment to the definition of PHI to exclude eligibility, enrollment, and premium payment data collected and held by or on behalf of an employer or plan sponsor. This information should be defined to include names, addresses, dependent information, and the names of the local union and contributing employer provided that none of this information is linked with claims data.

Consistent with the proposed modification discussed above to exclude “employment records” from the definition of PHI, the Department should expand the exclusion from PHI to include not only employment records but also eligibility, enrollment, and premium payment information collected and held by an employer or plan sponsor.

In addition, the Department should clarify that when a multiemployer plan (or other plan sponsor) maintains an eligibility and enrollment database, information from that database may be used or disclosed without consent or authorization for purposes related to eligibility, enrollment and premium payment.

2. Benefit Appeals Information

Background

As you know, the plan sponsor of a multiemployer group health plan is its Board of Trustees. Unlike employers who sponsor group health plans and often perform many plan administration functions, generally the only time that Trustees need access to PHI is when they decide benefit appeals. Even in a fully insured multiemployer plan, it is possible that Trustees may reserve the right under the plan documents to make the final decision regarding benefit claims and appeals.

Of course, this access can be achieved by taking advantage of the special group health plan rules contained in Section 164.504(f) of the Final Rule. Alternatively, the trustees could seek individual authorization for the use or disclosure of PHI for purpose of the appeal.

However, some Boards of Trustees currently decide appeals using claims records that have been redacted. In other words, certain personal identifiers have been removed, such as the individual’s name, address, telephone and fax number, e-mail address, social security number and other identifying information (e.g., local union number and employer’s name and EIN, unless relevant because of the benefit structure), date of birth (although age in years and months is used, if relevant), and retiree/active status (unless relevant because of the benefit structure). Often the name of the provider is also redacted, although the type of provider (e.g., hospital, laboratory, etc.) may be relevant.

In certain instances, a multiemployer plan may cover employees in an industry or a region, but may offer different benefit structures (and different contribution levels) for

employees of particular employers or local unions. Therefore knowing through which employer or local union the participant became eligible for benefits might be relevant to the level or type of benefits to which the participant was entitled.

Relevant Sections of the Privacy Rule

Section 164.501 of the Privacy Rule (as quoted above) defines “protected health information.” The type of redacted information used to decide appeals by many multiemployer group health plan trustees remains PHI under that definition even though key personal identifiers have been removed.

A covered entity may de-identify information that would otherwise be PHI. If the information is de-identified, it is no longer considered PHI and may be used and disclosed freely. This process is described at Section 164.514(a)-(c) of the Privacy Rule:

- (a) *Standard: de-identification of protected health information.* Health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual is not individually identifiable health information.
- (b) *Implementation specifications: requirements for de-identification of protected health information.* A covered entity may determine that health information is not individually identifiable health information only if:
 - (1) A person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable:
 - (i) Applying such principles and methods, determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information by an anticipated recipient to identify an individual who is a subject of the information, and
 - (ii) Documents the methods and results of the analysis that justify such a determination; or
 - (2) (i) The following identifiers of the individual or of relatives, employers or of household members of the individual are removed:
 - (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 ...:
- (C) All elements of dates (except year) for dates directly related to the 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, ...;
- (D) Telephone numbers;
- (E) Fax numbers;
- (F) Electronic mail addresses;
- (G) Social Security numbers
- (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, and

- (ii) The covered entity does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.

However, the redacted information used by the Trustees to decide appeals (as described above) does not appear to fall into the safe harbor of Section 164.514(b)(2), primarily because at times the Trustees do need to have some identifying information (such as local union number), if it is relevant to the appropriate benefit structure) and because we do not know what type of identifier the Department would consider to fall into Section 164.514(b)(2) (R).

If the Trustees need access to PHI to decide appeals and cannot perform this function with de-identified information, they can take advantage of the special group health plan rules found in Section 164.504(f) of the Privacy Rule. Among other things, these rules require that the plan sponsor certify that plan documents have been amended to incorporate provisions (1) to describe the intended uses of PHI (e.g., to decide benefit appeals) by the Trustees, (2) to require that the neither the plan sponsor, nor its employees or subcontractors, will use or disclose PHI in ways that a covered entity could not under the Final Rule and (3) to state that the plan sponsor will refrain from using PHI it obtains from the group health plan, health insurance issuer or HMO for employment-related purposes or in connection with other benefits or benefit plans.

If Trustees receive PHI from the group health plan in accordance with the special group health plan rules, they may only receive the minimum necessary PHI to accomplish the purpose for which the PHI was sought: to decide the benefit appeal. The minimum necessary requirements are found in Section Section 164.514(d) of the Privacy Rule.

Alternatively, Trustees could ask each individual who files an appeal of an adverse benefit determination to sign an individual authorization. The rules governing individual authorizations are found in Section 164.508 of the Privacy Rule.

NPRM Background:

The NPRM simplifies and clarifies the safe harbor for de-identified information. The Department notes that many commenters were concerned about the stringency of the safe harbor in the context of using individually identifiable information for research. 67 Fed. Reg. 14799 (March 27, 2002). The Department commented that although it wanted stringent standards for determining when personal medical information may flow unprotected, it also wanted the standards to be flexible enough so that the Privacy Rule would not be a disincentive for covered entities to use or disclose de-identified information wherever possible. 76 Fed. Reg. at 1498-99.

Therefore, the Department requested comments on:

... an alternative approach that would permit uses and disclosures of a limited data set which does not include facially identifiable information but in which certain identifiers would remain. The Department is not considering disclosure of any such limited data set for general purposes, but rather is considering permitting disclosure of such information for research, public health, and health care operations purposes.

The limited data set would not include the following information which the Department considers direct identifiers: name, street address, telephone and fax numbers, e-mail address, social security number, certificate/license number, vehicle identifiers and serial numbers, ULRs and IP addresses, and full face photos and any other comparable images. The limited data set would include the following identifiable information: admission, discharge, and service dates; date of death; age (including age 90 or over); and five-digit zip code.

...

In addition, to further protect privacy, the Department would propose to condition the disclosure of the limited data set on covered entities obtaining from the recipients a data use or similar agreement, in which the recipient would agree to limit the use of the limited data set to the specified purposes in the Privacy Rule, and limit who can use and receive the data, as well as agree not to re-identify the data or contact the individuals.

67 Fed. Reg. at 14799-800.

Discussion:

We think that the Department's suggestion for an alternative approach to the safe harbor for de-identified information has considerable merit. If Trustees could receive the type of information that the Department proposes to be included in the limited data set, they most likely could carry out their benefit appeals functions in connection with the health care operations of the multiemployer group health plan without needing any additional personal information.

In addition, we believe that Trustees would be willing to agree to limit the uses of the information in the limited data set along the lines that the Department is considering.

Alternatively, to deal with the concerns that Trustees have regarding whether the redacted information described above would meet the minimum necessary standard were the multiemployer plan to use the special group health rules, we suggest that the Department could clarify that these redactions would be a reasonable way to meet the minimum necessary standard.

Moreover, the Department could determine that if the only information that a plan sponsor received was the limited data set as described in the NPRM, the group health

plan could disclose that information to the plan sponsor without amending the plan documents as required under Section 164.504(f) of the Privacy Rule.

3. Model Authorization Form

Background:

Covered entities may use or disclose PHI with the authorization of the individual who is the subject of the PHI.

Discussion:

One of the most helpful features of the NPRM is the model business associate contract. The approach of providing model language for forms or other documents that many, if not most, covered entities will need is very helpful in assuring compliance with the Privacy Rule.

In the NPRM, the Department simplified and consolidated the requirements for individual authorization, eliminating, for example, the special requirements for authorizations for research. 67 Fed. Reg. at 14795. The Department is proposing a single set of requirements that generally apply to all types of authorizations. Id.

We strongly urge the Department to issue a model authorization form when it finalizes the proposed modifications to the Privacy Rule. This would result in a substantial reduction in cost to covered entities because each covered entity would otherwise have to create its own authorization form if it chose to use one. Issuance of a model authorization form would be a welcome form of guidance from the Department.

Conclusion

We appreciate this opportunity to comment on the proposed modifications to the Privacy Rule. If you have any questions, please feel free to contact me at (202) 737-5315 or by e-mail at rdefrehn@nccmp.org. We look forward to working with you.

Sincerely,

Randy G. DeFrehn
Executive Director