NATIONAL COORDINATING COMMITTEE FOR MULTIEMPLOYER PLANS

815 16TH STREET, N.W., WASHINGTON, DC 20006 • PHONE 202-737-5315 • FAX 202-737-1308

MARK H. AYERS
CHAIRMAN

RANDY G. DEFREHN
EXECUTIVE DIRECTOR
E-MAIL: RDEFREHN@NCCMP.ORG

August 1, 2011

Submitted via: http://www.regulations.gov
Keyword: RIN 0991-AB62

U.S. Department of Health and Human Services
Office for Civil Rights
Attention: HIPAA Privacy Rule Accounting of Disclosures
Hubert H. Humphrey Building, Room 509F
200 Independence Avenue, SW
Washington, DC 20201

Re: RIN 0991-AB62

To Whom It May Concern:

The National Coordinating Committee for Multiemployer Plans (the NCCMP) is pleased to submit these comments to the proposed rule issued by the Office for Civil Rights (OCR) modifying the HIPAA privacy rule's standard for accounting of disclosures of protected health information (PHI), published May 31, 2011 at http://www.gpo.gov/fdsys/pkg/FR-2011-05-31/pdf/2011-13297.pdf .

The NCCMP is the only national organization devoted exclusively to protecting the interests of the approximately 26 million workers, retirees, and their families who rely on multiemployer plans for health, retirement and other benefits. The NCCMP's 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, non-partisan organization, with members, plans, and plan sponsors in every major segment of the multiemployer plan universe, including in the airline, building and construction, entertainment, health care, hospitality, longshore, manufacturing, mining, retail food, service and trucking industries.

Multiemployer plans are established and maintained pursuant to collective bargaining agreements between one or more unions and at least two employers. Typically structured in accordance with section 302(c)(5) and (c)(6) of the Taft-Hartley Act, the plans are operated through stand-alone trusts managed by a joint labor-management Board of Trustees.

Multiemployer plans are typically self-insured and may rely on third party administrators (TPAs) and other business associates (e.g., pharmacy benefit managers and outside entities for dental or vision benefits) to administer their benefits. Others are self-administered, at least with respect to some of the health benefits they offer. The in-house information technology systems used by multiemployer plans range from older proprietary/custom systems to more modern systems supported by commercial developers.

Overview of Comments

In general, the NCCMP supports most of the proposed changes to the accounting requirement itself. However, the NCCMP does not support the proposal to require all covered entities to provide access reports to individuals who request them due to the burden that it will likely impose on multiemployer plans relative to the limited benefit that it would provide to plan participants.

The Existing Accounting Requirement

Under the HIPAA privacy rule, an individual has the right to request a covered entity to provide an "accounting" of certain disclosures of protected health information (PHI). This obligation applies to disclosures to people/entities outside the covered entity – for example, if a covered entity responds to a subpoena, it must keep a record of that response and produce it to the individual if requested to do so. The accounting of disclosures rule does *not* apply to use and disclosure of PHI by the Fund for routine plan administration purposes. Disclosures for treatment, payment[1], and health care operations[2] (TPO) purposes – the purposes for which multiemployer plans typically use and disclose PHI – are **not** currently subject to the accounting requirement. In our experience, it is rare for individuals to exercise this right to an accounting.

The Health Information Technology for Economic and Clinical Health (HITECH) Act

The Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted in 2009, required covered entities to include treatment, payment, and health care operations (TPO) disclosures from an "electronic health record" (EHR) when they were asked for an accounting of disclosures. EHRs are electronic clinical medical records created and maintained by health care providers. Multiemployer plans would not generally have an EHR because they are not engaged in providing treatment.

The Proposed Rule

The proposed rule changes the existing accounting requirement by:

- Limiting accountings of disclosure to PHI contained in a Designated Record Set (DRS)[3],
- Shortening the look-back time to compile and document disclosures to three years (now it covers the six years prior to the request for an accounting), and
- Eliminating some types of disclosures from the accounting requirement (e.g., disclosures for research purposes).

[1] "Payment" purposes relate to the adjudication of claims, and include eligibility, determinations of coverage, claims processing, payment and adjudication, and appeals.

[2] "Health care operations" purposes relate to the business operations of the plan, and include quality assessment, auditing functions, legal services, business planning and development, and business management.

[3] A designated record set includes medical and billing records that providers have, as well as enrollment, payment, claims, and medical management systems maintained by health plans and other records that are used to make decisions about individuals.

These are positive developments which the NCCMP supports. The NCCMP also supports the reorganization of the standard so that it lists which disclosures are subject to the requirement rather than which are not.

However, the proposed rule also includes certain requirements that multiemployer plans and other covered entities may have difficulty meeting. Specifically, the rule shortens the time deadline for providing the accounting from 60 days to 30 days (subject to one 30-day extension). We suggest that the 60 day requirement should be maintained.

The most troubling aspect of the proposed rule is the new right to an access report, which applies to PHI in an electronic Designated Record Set (eDRS). In our view, this new right unnecessarily expands upon what HITECH intended by:

- Broadening the scope of information to be accounted for to PHI in an eDRS. Under HITECH, the expanded accounting right applies only to the smaller subset of Electronic Health Records maintained by clinical health care providers, not by health plans, and
- Broadening the scope of information subject to the requirement to include *uses and disclosures.* The original accounting rule only applies to disclosures to people outside the covered entity.

If requested by an individual, the access report must cover the 3-year period prior to the request and include:

- date of access,
- time of access,
- name of the user accessing the eDRS, which should be the name of a natural person, if available, otherwise name of entity accessing the eDRS,
- description of what information was accessed, if available, and
- description of action by the user, if available, e.g., "create," "modify," "access," or "delete."

Concerns with the Access Report

The preamble to the proposed rule asserts that the new right to an access report builds on what the HIPAA security rule already requires. The HIPAA security rule requires covered entities to "implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports." (See §164.308(a)(1)(ii)(D).) It also requires covered entities to "implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information." (See §164.312(b).) The leap from these standards to the proposed access report for individuals is larger than that suggested by the preamble.

Creating the access reports would impose a potentially substantial burden on many multiemployer plans. How burdensome the requirement would be would vary depending on their systems' particular capabilities. Multiemployer plans' IT systems have a wide range of

capabilities, ranging from older proprietary/custom systems to more modern systems supported by commercial developers. Many systems have audit capability to track date/time of access plus user id (the three required categories). However, we have identified certain problems in expanding the access report requirement, including the following:

- Some systems are set to capture the required audit information only if the record is changed (not if it is accessed read-only).
- This type of data takes up a great deal of system memory. Because storing this data can greatly hinder system performance, many systems limit what they record or purge the data frequently (every three to six months or so) after the logs have been reviewed for suspicious activity or anomalies. Typically, the data would not be kept for three years, as the proposed rule would require.
- The process of translating the logs into some readable format understandable to individuals is labor intensive.
- The undue administrative burden of having to compile audit log data from multiple business associates – as noted in the comments submitted by the Entertainment Industry Health Plan [resemtimplementing either a manual or automated tracking: *"plan[s] could require all business associates to submit access report data on a monthly basis, maintain that data for three years, and generate reports from that data upon request. This would effectively require creation of a significant new health care data infrastructure that would ensure that access report data was formatted and standardized among all health plans and business associates. Absent this new infrastructure, we are not sure how all health plans and their business associates would manage the task of pulling a standardized and workable set of data from a network of very different, very complex IT systems."*

We question the value of the information that would be provided in an access report, particularly given the burden of tracking, retaining, and translating the raw data. Fund Administrators report having **never** received requests for an Accounting of Disclosure from a participant, raising serious questions about the cost/benefit of these additional requirements. Other parts of the security rule require plans to determine which employees may access which screens or modules containing ePHI and to have technical safeguards to implement those determinations. (See §164.308(a)(4)(i) – information access management; §164.312(a)(1) – access control.) As a result, telling a participant that Employee A vs. Employee B handled this particular transaction (e.g., an eligibility update) does not provide valuable information to the participant. This is especially true in smaller plan offices where all employees are likely cross-trained and authorized to handle all necessary transactions. Moreover, even if no plan participant ever requested such a report, the plan and its business associates would have to spend precious resources in an effort to upgrade systems and memory capacity just in case one individual came forward with such a request.

In summary, we suggest that the access report requirement be eliminated because the burden that it will likely impose on multiemployer plans greatly outweighs the limited benefit that it would provide to plan participants.

Conclusion

We appreciate the opportunity to submit comments on this proposed rule. Please do not hesitate to contact me if you have any questions about our comments or need additional information.

Respectfully submitted,

Randy G. DeFrehn
Executive Director