August 1, 2011

Submitted electronically via http://regulations.gov

United States 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

Attention: RIN 0991-AB62

Re: HIPAA Privacy Rule Accounting of Disclosures under HITECH

Dear Sir or Madam:

We are writing to provide comments on behalf of the American Benefits Council ("Council") and the United States Chamber of Commerce (the "Chamber") regarding the notice of proposed rulemaking ("Proposed Rule") issued by the Department of Health and Human Services (HHS) at 76 Fed. Reg. 31426 (May 31, 2011), to modify the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") Privacy Rule's standard for accounting of disclosures of protected health information.

The Council is a public policy organization representing principally Fortune 500 companies and other organizations that assist employers of all sizes in providing benefits to employees. Collectively, the Council's members either sponsor directly or provide services to health and retirement plans that cover more than 100 million Americans.

The Chamber is the world's largest business federation, representing more than three million businesses and organizations of every size, sector, and region. More than 96 percent of the Chamber's members are small businesses with 100 or fewer

employees, 70 percent of which have 10 or fewer employees. Yet, virtually all of the nation's largest companies are also active members. The Chamber is particularly cognizant of the problems of smaller businesses, as well as issues facing the business community at large. Besides representing a cross-section of the American business community in terms of number of employees, the Chamber represents a wide management spectrum by type of business and location. Each major classification of American business—manufacturing, retailing, services, construction, wholesaling, and finance—is represented.

BACKGROUND AND SUMMARY

In 2009, the Health Information Technology for Economic and Clinical Health Act ("the HITECH Act" or "the Act") was enacted, in part, to require covered entities and business associates to account for certain disclosures of protected health information ("PHI") to carry out treatment, payment, and health care operations. Section 13405(c) the Act[1] provides that the exemption at § 164.528(a)(1)(i) of the Privacy Rule for disclosures to carry out treatment, payment, and health care operations no longer applies to disclosures "through an electronic health record." Under section 13405(c), an individual has a right to receive an accounting of such disclosures made during the three years prior to the request.

The proposed modifications to the Privacy Rule are intended, in part, to implement this statutory requirement. However, in addition, relying on "its more general authority under HIPAA," the Department "has proposed to expand the accounting provision to provide individuals with the right to receive an access report indicating who has accessed electronic protected health information in a designated record set."

This proposed regulatory expansion significantly enlarges the scope of changes that were contemplated by the Act, in a manner that greatly adds to the burden of the accounting requirement. First, it would significantly expand the Act to require covered entities to account for both disclosures and internal uses of information for purposes of treatment, payment and health care operations. It would also greatly expand upon the language of the Act by requiring an accounting for disclosures of (and access to) all electronic PHI ("EPHI") that is part of a "designated record set," a much wider range of PHI than the PHI that is contained within an electronic health record. The burden of this expansion is heightened by other revisions proposed by the Department, which include a shorter deadline, mandated coordination with business associates to respond to individual requests within that time frame, and an inexplicable requirement to

[1] Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA) Pub. L. 111–5),

accommodate requests by individuals to provide information in a specifically designated format.

The Council and the Chamber appreciate the Agency's efforts to clarify and, in some cases, simplify the accounting requirements for disclosures that are not made for purposes of treatment, payment and health care operations, under 45 C.F.R. § 164.528(a). Notwithstanding, the Proposed Rule raises a host of issues and concerns for our members. Perhaps most importantly, the Proposed Rule significantly expands the scope of the accounting rule to encompass far more frequent and routine uses and disclosures of EPHI. Our comments with respect to the Proposed Rule are set forth below.

ACCESS REPORT FOR ELECTRONIC PHI

The HITECH Act expanded the accounting rule only for "electronic health records" ("EHRs"), which are defined under Section 13400 of the HITECH Act as "an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by *authorized health care clinicians and staff*." (Emphasis added.) An "EHR," as envisioned under this definition, would likely function as a single, unified clinical record maintained by a health care provider with respect to an individual. This is made clear through other provisions of the HITECH Act that pertain to EHRs:

- Section 3000(1) (42 USC 300jj) defines "certified EHR technology as a qualified electronic health record that is certified pursuant to section 3001(c)(5) as meeting standards adopted under section 3004 that are applicable to the type of record involved (as determined by the Secretary, such as an *ambulatory electronic health record for office-based physicians or an inpatient hospital electronic health record for hospitals*)." (Emphasis added.)

- Section 3000(13) defines a qualified electronic health record as "an electronic record of health-related information on an individual" that includes "patient demographic and clinical health information, such as medical history and problem lists," and that can be used, among other things, to "provide clinical decision support" as well as "support for physician order entry."

The notion inherent in the statutory language is that requiring an accounting for disclosures that are made for routine health care related purposes would be relatively less burdensome when they are made through such a unified record.

The Proposed Rule, however, extends the access report requirement to all electronic PHI that is part of a "designated record set," as defined by the Privacy Rule, and further expands the rule to include all access (even internal) to such EPHI:

> While the HITECH Act provision only addresses "disclosures" and refers to an EHR, we are exercising our discretion under the more general HIPAA statute to expand this right to uses of information (*e.g.*, electronic access by members of a covered entity's or business associate's workforce) and to all electronic protected health information about an individual in any designated record set.[2]

First, while HHS states that it is limiting the access report only to include information in a designated record set, this is itself a significant expansion over what was originally intended by Congress. A "designated record set" is defined under the Privacy Rule as "a record used to make decisions about individuals, including all enrollment, payment, and claims adjudication records," or, as HHS puts it, "the medical and health care payment records maintained by or for a covered entity, and other records used by or for the covered entity to make decisions about individuals."[3]

Expanding the accounting requirement to cover access to all electronic records maintained in designated record sets by all covered entities (even those that do not maintain electronic health records) is unduly burdensome and very costly. It would require all covered entities to query nearly every system they maintain for the full range of activities that are likely to generate a relatively high volume of requests for information, for instance, claims records maintained by a health plan, or billing records maintained by a health care provider.

HHS acknowledges repeatedly that it has gone beyond the scope of the HITECH Act's statutory language, but says it feels the expansion is "reasonable." However, the specific justifications given for such a wide ranging expansion of the accounting requirement are unpersuasive.

HHS largely justifies expanding the accounting requirement to all EPHI because covered entities are already required by the security standards of 45 C.F.R. § 164.302 *et seq*. (the "Security Rule") to maintain an access or audit log, that is, "the raw data that an electronic system containing protected health information collects each time a user … accesses information."[4] However, access logs typically are in code format and not necessarily easy to obtain quickly for a period as long as three years. This point is understood by HHS, when it notes that an "access report" would be the document that a system administrator or other appropriate person would generate from an access log in a format that is understandable to the individual.[5] Thus, even if access logs can be readily and timely obtained, they would need to be translated, sorted, and compiled to

---

[2] (76 Fed. Reg. 31436)

[3] 76 Fed. Reg. 31430

[4] 76 Fed. Reg. 31436

[5] *Id.*

meet a single participant's request. Converting these access logs to reports that are limited to, and understandable by, individuals will require considerable personnel and programming resources by covered entities.

Indeed, HHS appears to recognize that access logs are not designed to provide the kind of accounting originally contemplated under the Privacy Rule for external disclosures that are not related to treatment, payment or health care operations. Hence, while it requires the covered entity to provide an access report, it has declined to require that the access report "include a description of what information in the electronic designated record set was accessed," if that information is not "available."[6] Thus, as HHS concedes elsewhere, the kind of report it contemplates is actually quite burdensome to provide, and the only interest being met through this requirement is knowledge of "who" accessed information, not what information was accessed, or for what reason.

> As noted earlier, we recognize that electronic designated record set information will often reside in a number of distinct systems that maintain separate access logs. There may be significant burden in aggregating this data into a single access report. However, we believe that this administrative burden is reasonable in light of the interests of individuals in learning *who* has accessed their protected health information.[7] (Emphasis added).

Contrary to HHS's assertion, as we discuss further below, knowing "who" accessed information is unlikely to provide the individual with meaningful information to protect legitimate interests, and cannot justify such a sweeping expansion of accounting rights.

HHS justifies the reasonableness of requiring an accounting for "uses" and not just "disclosures" by stating that most covered entities that responded to its previous requests for information indicated that "their system is unable to automatically distinguish between uses and disclosures of information."[8] Hence, HHS concludes, "the inclusion of all access, rather than only access that represents a disclosure, may actually be less burdensome on covered entities and business associates than the alternative of configuring systems to distinguish between uses and disclosures of information."[9]

---

[6] *See* 76 Fed. Reg. at 31438

[7] 76 Fed. Reg. 31439

[8] 76 Fed. Reg. 31437.

[9] 76 Fed. Reg. 31437-38

HHS's Proposed Rule will not be "less" burdensome to those entities that do have electronic systems with the capability to efficiently distinguish "disclosures" from "access," automatically or not. Moreover, even if the covered entity/business associate systems cannot distinguish between internal access and external disclosure, this fact does not justify the expansion of the requirement to track access by all electronic systems (not just EHRs) for all transactions that may take place electronically.

With respect specifically to EHRs, if in fact an entity would find it more burdensome to distinguish access from disclosures, HHS could easily meet such an objection by permitting, not requiring, the entity to meet its obligations by providing information on both access and disclosures.

For the foregoing reasons, the Council and the Chamber respectfully request that future guidance make clear that covered entities/business associates are only required to provide an accounting with respect to disclosures (not uses) through EHRs.

ADDITIONAL ASPECTS OF THE PROPOSED MODIFICATIONS

The Proposed Rule compounds the complexity and added burden of accounting related to treatment, payment and health care operations by extending it to include not only disclosures to external parties, but access *by name* by any individual, as well as coordination among covered entities and potentially multiple business associates to address an individual's request through a single response that eliminates any duplication, and that must be delivered in any feasible format that is requested by the individual. These expanded duties are also supposed to be completed in the shorter timeframe proposed by the modified rule. Our additional comments with respect to these and other aspects of the Proposed Rule are below.

Access Report to Include Names

As stated above, HHS asserts in several places in the Proposed Rule that an individual has an interest in knowing *who* has accessed their information. Therefore, the Department proposes to require that access reports include the actual names of those individuals who have accessed the individual's PHI. We do not believe there is any policy rationale for requiring the disclosure of the names of individuals who have accessed information, presumptively for legitimate business purposes.

We recognize that there have been some high profile cases in which PHI was accessed by unauthorized individuals. With respect to most organizations, however, merely stating the name of the person who accessed information is unlikely to provide individuals with any insight into how or why information is being used, even where such violations might have occurred. An individual would be unable to determine whether an employee's access to information raises any questions or concerns unless

they actually know the person and their role within the covered entity or business associate. In addition, while perhaps not of paramount concern to HHS, disclosing names of employees of covered entities or business associates whose access to PHI was presumptively legitimate provides an opportunity for contact that is neither warranted by circumstances, nor likely to be constructive.

In short, the Security Rule (access and user controls) provides the core protection against unauthorized access to or misuse of PHI. Requiring a report of names in all cases where an accounting is requested significantly adds to the burden of the accounting requirement to a degree that cannot be justified by the random and insignificant number of cases in which an individual would actually be able to use an accounting as a means of identifying unauthorized access, or on the basis of any other articulated policy rationale. Thus, for the foregoing reasons, we request that covered entities only be required to address unauthorized disclosures of PHI.

Access Report to Include Business Associates

The HITECH Act expressly stated that, under the new EHR accounting rule, a covered entity could either compile a single report of disclosures by both the covered entity and business associate, or could compile its own report and refer individuals to the applicable business associate for an EHR accounting from that business associate. The Proposed Rule apparently rejects the express language of the HITECH Act and requires the covered entity to compile a single report that includes any access to electronic PHI by both the covered entity and business associate. HHS says it knows that this requirement is beyond what is required in HITECH, but is "exercising our general authority under the HIPAA statute . . ." to make the expansion. In addition, the Proposed Rule provides that the access report must be aggregated so each access is only listed once (where there may be multiple systems from the covered entity and business associate).

HHS provides no justification for expressly rejecting the statutory language in favor of its own general authority. Moreover, HHS is ignoring the new regime under the HITECH Act which directly imposes statutory obligations on business associates and subjects them to the penalties for their own violations of the statute. As has been pointed out with regard to other aspects of the Privacy Rule, many business associates are larger than the covered entity itself. Furthermore, many business associates contract with many different covered entities, and a single covered entity typically has multiple business associates. This is especially likely to be the case for group health plans, in particular, which often carry out virtually all of their operations through large business associates that are covered entities in their own right. These business associates maintain the electronic systems and other data capabilities that must be queried to respond to the request for an accounting by a health plan participant, as well as the staffing and resources to carry out such requests. It is not reasonable to put the burden of responding to such a request on hundreds or even thousands of group health plans,

for purposes of ensuring the responsiveness of their much more sophisticated business associate vendors.

Requiring all covered entities to "coordinate with" or take responsibility for accounting for disclosures and access with respect to every business associate deprives both covered entities and business associates of the flexibility to structure compliance with the accounting rule in a manner that was contemplated by Congress, and that is most likely to be convenient and efficient for both themselves and the individual whose information is the subject of the request. Accordingly, we request that covered entities again be permitted to elect, at their discretion, to compile a single report of disclosures or, alternatively, refer individuals to an applicable business associate for an EHR accounting from that business associate.

Deadline for Providing an Accounting

The Proposed Rule shortens the time period to provide an accounting from 60 days to 30 days (plus a 30-day extension). This means that a health plan must review and translate its own access log and coordinate and compile the access logs from all business associates to create an understandable report within 30 days. In addition, the individual can specify the format (*e.g.*, software) the report must be in, so each report will have to be customized for each request.

There does not seem to be a strong policy reason for shortening this time, particularly when some aspects of the accounting rule would be more difficult, such as compiling business associate disclosures and providing the accounting in the format requested by the individual (see below). Additionally, it is noteworthy that the time periods for the right to access and amend PHI remain at 60 days. Accordingly, we request that the original 60-day time period be reinstated in lieu of the 30-day time period set forth in the Proposed Rule.

Customized Format

The Proposed Rule requires the accounting to be provided in a format requested by the individual "if readily producible." The Preamble says this means that the individual may request the accounting in PDF form or in a particular software. Therefore, in addition to providing the report, plans must also customize it for each individual, in a shorter time period as required by the Proposed Rule. The purpose of an accounting is to provide a record to individuals of disclosures of their PHI. So long as the report conveys that information in a format that is understandable and usable and (e.g., a report should not be in computer code that is unintelligible to the average person), we fail to see what additional legitimate policy is served by customizing a report for an individual's specific intended use for the information.

Effective Date

The Proposed Rule has a confusing effective date, which varies depending on when a record was acquired. For records acquired on or after January 1, 2009, the effective date is January 1, 2013. For records acquired before January 1, 2009, the effective date is January 1, 2014.

The effective date is loosely based on the effective dates listed in the HITECH Act, but those effective dates only apply to EHR accounting – not the expansive new access report of all electronic PHI, which is not included in the HITECH Act at all. Even then, the HITECH Act gave HHS the discretion to extend some of these dates to 2016, which HHS did not do.

For ease of administration and minimize confusion, we request that the effective date for *all* records subject to the rule (*i.e.*, whether acquired before or after January 1, 2009), be *no earlier than January 1, 2014*. This would provide important clarity regarding application of these new rules and ensure that all parties have sufficient time to implement the changes. We believe this timeframe is also warranted to allow interested parties and the Agency to consider whether or how the accounting disclosure requirements may apply to data sharing related to Health Exchanges that are to be established by 2014 under the Patient Protection and Affordable Care Act (PPACA).

* * *

Thank you for the opportunity to comment on the Proposed Rule and for considering our recommendations. We look forward to working with you on these important issues. If you have any questions or would like to discuss these comments further, please contact the undersigned.

Sincerely,

Kathryn Wilber
Senior Counsel, Health Policy
American Benefits Council
(202) 289-6700

Katie Mahoney
Director, Health Care Regulations
U.S. Chamber of Commerce
(202) 463-5825