

Filed via online portal

August 1, 2011

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-AB-62

To Whom It May Concern:

BITS¹, the technology policy division of The Financial Services Roundtable, and the American Bankers Association² (collectively referred to as the “Associations”) appreciates the opportunity to provide comment to the Department of Health and Human Services (“Department”) on “HIPAA Privacy Rule Accounting of Disclosures Under the Health Information Technology for Economic and Clinical Health (HITECH) Act.”

The HITECH Act provided an incentive to the health industry to adopt electronic health record systems. It calls for a multitude of rulemakings aimed at strengthening the privacy and security protections for electronic health transactions. In addition, it requires the maintenance of different rules for other types of non-electronic health records and protected health information (PHI).

We recognize the Department’s effort to promulgate rules that implement the HITECH Act requirements regarding disclosures of electronic health records as we believe ensuring privacy is the responsibility of all participants in the marketplace, including consumers.

Our members have actively followed the development of HIPAA regulations. While basic financial institution services and activities are generally exempt from HIPAA pursuant to 42

¹ BITS addresses issues at the intersection of financial services, technology and public policy, where industry cooperation serves the public good, such as critical infrastructure protection, fraud prevention, and the safety of financial services. BITS is the technology policy division of The Financial Services Roundtable, which represents 100 of the largest integrated financial services companies providing banking, insurance, and investment products and services to the American consumer. For more information, <http://www.bits.org/>.

² The American Bankers Association represents banks of all sizes and charters and is the voice for the nation’s \$13 trillion banking industry and its 2 million employees. ABA’s extensive resources enhance the success of the nation’s banks and strengthen America’s economy and communities. Learn more at www.aba.com.

U.S.C. section 1320d-8³, certain financial institutions provide covered entities with more extensive financial services requiring them to comply with many aspects of HIPAA as a result of their relationships as business associates. In addition, financial institutions may offer products, such as insurance and third-party administration services for covered entity health plans which make them covered entities.

While the Associations support the Department's effort to implement HITECH's requirements effectively, we offer the following suggestions regarding the accounting of disclosures and access reports for the Department's consideration. Specifically, we believe the notice of proposed rulemaking (NPRM) raises five significant concerns and challenges for financial institutions that are business associates or covered entities, which we summarize below and subsequently discuss throughout the following sections.

- The proposal's designated record set significantly broadens the scope of the requirement for an accounting of disclosures beyond the HITECH Act's Electronic Health Record (EHR).
- The 30-day requirement to provide a personalized accounting to an individual consumer does not offer business associates or covered entities adequate time to prepare a response for either the covered entity client through which a request originated or the individual making the request.
- HITECH does not expressly authorize the Department to create a new right to receive or an obligation by the covered entity to provide an access report for electronic PHI.
- The Department does not identify any significant or compelling consumer benefit that counterbalances the enormous cost business associates would incur to modify existing systems and processes to account for access at an individual consumer level.
- The proposed access report provisions introduce a level of complexity that would likely lead to individual consumer confusion and frustration.

Accounting of Disclosure

The current accounting rule, 45 C.F.R. 164.528, provides individuals with the right to seek an accounting of disclosures of the individual's PHI. A disclosure is defined as "the release, transfer, provision of, access to, or divulging in any other manner of information outside the entity holding the information." The current rule exempts disclosure regarding treatment, payment, and health care operations. The HITECH Act is very clear that an accounting for treatment, payment, and health care operations is only applicable to EHR. We believe the Department has exceeded its authority under the HITECH Act by expanding the disclosure requirement to "protected health information in an electronic designated record set," which has a much broader meaning. This expanded requirement for disclosure places a significant burden on financial institutions acting as business associates as many of the services provided by financial institutions are related to payment and health care operations, but not to EHR.

Covered entities and business associates will incur significant burdens as a result of a number of requirements in the proposal. For example, the proposal's requirement permitting

³ 42 U.S.C. section 1320d-8 provides that HIPAA does not apply to an institution to the extent that it is engaging in certain activities, such as authorizing, settling, processing or reconciling payments.

individuals to request the accounting in the form and format of their choosing creates additional unnecessary burdens on institutions. Covered entities and business associates will be able to develop some standard processes for gathering data, but will be unable to develop a completely automated report as the end product must include a manual portion to customize data to an individual's request and ensure all information is included. For financial institutions that generally manage PHI at a covered entity client level rather than an individual level, the technical and system constraints of producing an accounting in that fashion would be impracticable. We believe institutions should be able to provide their own form for this request, as long as all requisite information is included.

In addition, covered entities and business associates will incur significant \burdens to renegotiate or amend all existing business associate agreements. Moreover, they will need to implement policies, procedures and training to respond to and explain such disclosures to individuals.

Further, the proposed requirement for preparing an accounting for impermissible disclosures is in direct conflict with the breach notification rules that require notice only if there is a significant risk of financial, reputational, or other harm to the individual. The inclusion in the accounting of impermissible disclosures that do not raise significant risks of harm may lead to consumer frustration and confusion, in that individuals may see the accounting as a delayed notification of security breaches.

To reduce customer confusion, covered entities may begin to provide additional notice, or otherwise over-notify, which would dilute a consumer's sensitivity to disclosures wherein their information actually may suffer a significant risk of harm. Given the likelihood that an accounting of impermissible disclosures could lead to costly new processes and procedures for responding to consumer frustrations and inquiries, covered entities and business associates may broaden the instances where notification would be provided to the individuals. These new standards would require the renegotiation and amendment of business associate agreements at significant cost to both covered entities and business associates.

We agree with the Department's decision to list the types of disclosures expected from the requirement to provide an accounting. We believe it will result in a clearer rule for covered entities and business associates and assist in consumer understanding.

Access Reports

The proposed rule provides for an entirely new right for individuals to request a report listing all access to PHI in an electronic designated record set, including internal access to an individual's electronic designated record set. The Associations believe that the proposed rule goes beyond the action directed by the HITECH Act, as the Department recognized in the preamble to the proposal. The Department noted that its goal is to improve the workability and effectiveness of the current accounting requirements. We believe the proposed rule does not accomplish this goal and instead introduces counterproductive complexity, reduces effectiveness of the accounting requirements, and is extremely burdensome to covered entities and business associates.

To comply with HITECH, covered entities and business associates currently limit access to PHI to the minimum necessary; therefore any information provided in the access report would be very detailed and/or routine. There does not appear to be a compelling benefit to providing consumers with this level of detail considering that individuals have access and amendment rights under 164.524 and 164.526, are provided notice of the use and collection of their data through privacy notices, and are notified when unauthorized access or disclosures creates a risk of harm.

The Department states that it believes individuals are interested in learning who has accessed their information even if the access is internal, by an organization's workforce members. It is not clear why the Department holds this belief. To the contrary, the responses to the Department's request for input that the NPRM summarizes⁴ do not appear to support that conclusion. Instead, the Department's own NPRM indicates that the responses to its second and third requests for input show that while individuals are aware of their right to receive an accounting of disclosures, very few individuals exercised their ability to receive an accounting of disclosures. Given the lack of previous interest, it does not appear individuals would have a great interest in learning about who internally at an organization has accessed their information, particularly when individuals are aware that access is limited to the minimum necessary.

We believe that HIPAA's rules on data restriction and breach notification provide thorough coverage to ensure the privacy and security of an individual's health data, and an additional access report is unnecessary. HIPAA regulations restrict PHI usage and organizational access. In addition, HIPAA's data breach notification regulations require notification to individuals when their PHI is compromised in a manner that poses a significant risk of financial, reputational, or other harm to the individual, as defined in 45 C.F.R. Section 164.402. This includes notification of access by an internal workforce member when the access is in bad faith. We believe the addition of notice through access reports will create consumer confusion and frustration, which will create new administrative burdens on business associates and covered entities as previously discussed.

In addition, the requirement to include the individual's name who viewed the record could violate employees' privacy rights. The workforce of covered entities and business associates should have the ability to access files for legitimate business purposes as required to perform their job without fear that their personal information can/will be shared with consumers. We see no benefit, and great potential for harm, in providing their name in disclosure reports. To protect the rights of the workforce and to the extent that any report is provided, it should focus not on individual workforce members but on the organization and department (if available) that accessed the record.

We disagree with the Department's assessment that compliance would not be burdensome, because of the current monitoring requirements imposed on businesses associates and covered entities. However, the monitoring designed to comply with the current rule is for information security purposes only and is intended specifically to identify *unauthorized* access to PHI. However, the proposed requirements for the access report would require covered entities and business associates to also disclose *authorized* access to PHI. As we

⁴ See 31426 Fed. Reg. at 31427 – 31428.

mentioned earlier, most business associates do not maintain PHI at an individual level; providing an access report at an individual's request would likely be technically and administratively burdensome. To comply with this expanded requirement, our members would incur significant system development expenses, and be required to devote substantial resources to build a system to identify, track and report both authorized and unauthorized access. In many ways, the costs associated with compliance could lead financial institutions to reassess and reconsider offering any line of products, which would render them business associates.

In a similar vein, we strongly disagree with the Department's proposal to require the provision of information in designated record sets rather than EHRs, as specified in the HITECH Act. Our members in their business associate relationships would have far fewer, if any, EHRs in their possession as compared with electronic designated record sets. Focusing on electronic designated record sets greatly increases the burden on our members with no added privacy or other benefit to individuals.

Congress demonstrated its intention that the elimination of the treatment, payment, and operation exception for accounting disclosures, would be tied to EHRs. It provided monetary incentives for the use of EHRs while at the same time requiring recommendations on the use of EHR technology standards that would allow for an accounting of disclosures made for treatment, payment, and operations purposes. Congress was concerned with the burden that new accounting standards would require and took steps to try to ensure this burden would be mitigated. Congress also focused its privacy concerns on accounting of disclosures of EHRs and not designated record sets. This is logical given that an EHR would, by definition, contain information connected to "health care clinicians and staff," typically the most sensitive type of health information. In comparison, a designated record set is defined more broadly, and can encompass more routine health-related information, including payment information.

The Associations urge the Department not to adopt any requirements that call for the provision of an access report detailing internal access to PHI. Instead, the Department should exempt all disclosures for treatment, payment, and healthcare operation purposes except with respect to an EHR as Congress intended. We believe this will satisfy the intent of the HITECH Act's requirements and provide information of greatest interest to individuals, while avoiding unnecessary burden.

Nonetheless, if the Department proceeds with requirement for an access report, it should consider only limited exceptions for inclusion. Routine access limited to the minimum necessary to perform job functions should not be subject to any requirement to provide an access report. The Department should consider additional key activities that should be formally exempt from the accounting requirement, such as access by internal workforce members to assess access for purposes of audit and/or investigation of potential unauthorized access. For example, when an institution needs to investigate privacy events or conduct other activities of a sensitive nature. If this is reported to individuals, they may be confused to see information regarding a privacy event when their records were not part of the compromise. If an individual's records are part of the compromise and deemed to be at serious risk of harm to the consumer, s/he would have received the information through the traditional breach notification channels.

Generally, further exemptions from access and disclosure requirements should be considered for financial institutions if their receipt, access, use, or disclosure of PHI is performed at a covered entity level and not at the individual record level. Otherwise, financial institutions will be required to create individual level records solely for the purpose of providing accounting and access which creates a significant financial and resource burden and could actually increase the potential for unauthorized or impermissible disclosures.

Overall

Given the need to obtain and compile three years of data for individuals upon request and in their specified format for both the accounting of disclosures and access report, the reduction to a 30-day response time period is insufficient. The process for both reports will be highly manual and thus burdensome and operationally challenging. This is especially true in circumstances where a covered entity uses a business associate service provider and thus must request and retrieve the information from the service provider. Often, a covered entity uses several business associates, and business associates may have many subcontractor arrangements. We urge the Department to retain the original 60-day time period.

In addition, we support the Department's limitation of the period of disclosures for which an entity must account to a period of three years. This ensures that the more recent disclosures, which are likely to be of most interest to consumers, are accounted for, while eliminating unnecessary burden in accounting for older disclosures. We appreciate the reduction of the overall request period and urge the Department to make all requirements consistent at three years. Currently, the retention requirements are six years.

As previously mentioned, further exemptions for financial institutions should be considered as few if any of services provided by a financial institution maintain records required for an access report or an accounting of disclosures at an individual level.

When creating the final rule, we urge the Department to consider the increased amount of resources required for business associates and covered entities to comply with the final rule. This rule will require institutions to renegotiate business associate contracts, revise Notices of Privacy Practices, develop internal monitoring and tracking systems, and develop an internal system for manually creating each report based on the individual's unique requests.

If you have any questions or comments, please feel free to contact us as noted below.

Sincerely,



Paul Smocer
Acting BITS President
BITS
Financial Services Roundtable
202-589-2437
PaulS@fsround.org



Cristeena Naser
Senior Counsel, ABA
Center for Securities, Trust & Investment
American Bankers Association
202-663-5332
CNaser@aba.com