HIMSS Electronic Health Record Association

33 West Monroe Street
Suite 1700
Chicago, IL 60603

Phone: 252-946-3546
Fax: 734-973-6996
E-mail: himssEHRA@himss.org

August 1, 2011

Ms. Georgina Verdugo, JD
Office for Civil Rights
U.S. Department of Health and Human Services

Attention: HIPAA Privacy Rule Accounting for Disclosures

Submitted electronically at: http://www.regulations.gov

Dear Ms. Verdugo:

The Electronic Health Record (EHR) Association is a trade association of 42 electronic health record (EHR) companies that join together to lead the health IT industry in the accelerated adoption of electronic health records in hospital and ambulatory care settings in the US. We are pleased to respond to the Notice of Proposed Rule-Making (NPRM) on the HIPAA Privacy Rule related to Accounting for Disclosures. This response was developed through an open, collaborate process engaging representatives from our member companies that represent the majority of installed, operational EHRs in the US, and our customers who use them to improve the quality and efficiency of care delivery.

Summary

The EHR Association recognizes the importance of providing transparency to patients regarding how their health information is being accessed and disclosed by covered entities and business associates. The HITECH Act directs the Secretary of Health and Human Services (HHS) to promulgate regulations requiring covered entities to account for disclosures of electronic protected health information (ePHI), including those related to treatment, payment, and health care operations, which had been exempted from prior HIPAA Accounting for Disclosure requirements. HITECH also directs the Secretary to balance the burdens imposed on the covered entities with the rights of individuals to know about the disclosures of their ePHI.

The EHR Association supports a number of the proposed changes to current regulations about Accounting for Disclosures (as distinct from the proposed access reports), especially those intended to provide clarity and reduce burdens on healthcare providers. Listing the types of disclosures subject to the accounting requirement, rather than listing exemptions, and constraining the list to a manageable size, is one example that our Association believes will make it simpler for providers to comply. Additionally, we also applaud the recognition that reporting disclosures made during the process of electronic health information exchange (HIE) would be overly burdensome, while simultaneously not offering significant benefit to requesting individuals.

However, although we appreciate the responsiveness of the Office of Civil Rights (OCR) to many of the concerns that we previously conveyed regarding this issue, on balance, we do not believe that the proposal outlined in the NPRM, primarily with respect to the new concept of “access reports,” ultimately provides a reasonable balance between value to individuals and burden on covered entities and business associates. Our objective is to ultimately see requirements implemented related to disclosures that lead the provider and other covered entities to produce reports valuable

to individuals that exclude meaningless and redundant access points to ePHI. Therefore, we urge OCR to rethink and consider withdrawal of the access report proposal entirely, which appears to us to be unworkable on many levels. This concern with feasibility is particularly relevant to the proposals regarding the information required within the access report.

As explained in our detailed comments below, we believe that OCR has expanded its approach beyond what might be considered reasonable given the intent of the HITECH Act. Our primary concerns focus on the proposals regarding access reports as well as the requirement that the accounting for disclosures, and especially the access reports, be based on a designated record set (DRS) rather than an EHR, as specified by the applicable HITECH provision.

The 2002 HIPAA Privacy Rule defined a DRS very broadly and, in practice, a wide variance now exists among providers as to what data sets should be included within their DRS. Because of this ambiguity, OCR and consumer expectations may be at odds with individual providers' interpretation and understanding of what their DRSs should be. Additionally, contrary to statements in the NPRM, we believe that use of the DRS serves to expand rather than limit the impact of these requirements. Using the DRS as the basis of information to be included in access reports creates an undue burden on covered entities and business associates to collect and aggregate data from numerous health IT systems outside of the HITECH Act's intent that just the information contained within an EHR be used.

With respect to the revised approach to actual Accounting for Disclosures, we appreciate and generally agree with the OCR's proposed approach to specify a set of disclosure circumstances for which an accounting will be required.

Again, the EHR Association appreciates the opportunity to respond to this important NPRM and offers its help to OCR in further understanding the issues or concerns outlined in our detailed comments below.

Detailed Comments

[OCR] request[s] comment on [their] proposal to limit the accounting requirement to protected health information in a designated record set and whether there are unintended consequences with doing so either in terms of workability or the privacy interests of the individual. (31430)

The EHR Association recognizes and appreciates the intent of using the DRS[1] as a way to limit which information should be included within the accounting requirement. We believe, however, that using the DRS as the defined data set for this rule actually expands the accounting requirement beyond the focus of this regulation -- i.e., providing an accounting of the disclosures out of an EHR as authorized by the HITECH Act -- and extends it to other electronic systems that maintain portions of the DRS. This shift creates workflow issues and undue burden for covered entities that will have to aggregate data from their EHR(s) and other electronic systems to provide the required DRS.

Fundamentally, we believe that the DRS burden that is placed on covered entities to meet the access report requirement will also affect their ability to provide such reports in a timely, accurate, and meaningful fashion.

Given these concerns, we believe that OCR should look to the HITECH Act definitions of Electronic Health Record[2] and

[1] 45 CFR 164.501, **Designated record set** means: (1) A group of records maintained by or for a covered entity that is: (i) The medical records and billing records about individuals maintained by or for a covered health care provider; (ii) The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or (iii) Used, in whole or in part, by or for the covered entity to make decisions about individuals. (2) For purposes of this paragraph, the term record means any item, collection, or grouping of information that includes protected health information and is maintained, collected, used, or disseminated by or for a covered entity.

[2] HITECH Act, Section 13400 Definitions. (5) **Electronic Health Record**. - The term ''electronic health record'' means an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff.

Qualified Electronic Health Record[3] to limit the accounting requirement to only "an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff" and, if possible, to further bound this by use of the Qualified EHR definition, which is closer to actual practice.

[OCR does not] believe that it will be a significant detriment to individuals to reduce the accounting period from six years to three years. In contrast, we believe it is a significant burden on covered entities and business associates to maintain information on six years of disclosures, rather than three years. We request comment on this issue and if there are specific concerns regarding the need for accounting for disclosures beyond three years. (31430)

The EHR Association supports the reduction of the accounting period from six years to three years because we believe that information disclosed more than three years ago is likely of little relevance to an individual. However, it is worth pointing out that from a technical viewpoint, the amount of disk space and disk pathways needed to store even just three years of access data would be costly for a single covered entity, such as a hospital or hospital system. This cost could also be exacerbated depending on the level of "drill down" expected by the OCR – i.e., the more granular the expected reports (and thus the greater the volume of data the EHR must capture), the larger the storage requirements. Clarification here is clearly necessary.

Even under optimal circumstances, where providers can use certified EHR systems to perform name-specific and period-limited queries, access reports for a shorter period of time than the proposed three years could take several hours to generate. The time and resources required to generate the more complicated report that would be needed to satisfy the proposal across a full array of DRSs would obviously be much greater and place a larger burden – in cost and resources – on providers.

We note, too, that the timeline, which uses 2009 as a baseline date, is problematic for three reasons:

- First and most critically, it is based on HITECH statutory references to accountings of disclosure involving EHRs and not access reports relating to all DRSs.
- Second, the HITECH certification requirements placed Accounting for Disclosures within the optional category for Stage 1 meaningful use, and do not fully align with the proposed requirements within this regulation.
- And third, ancillary and departmental systems within healthcare enterprises do not follow the same robust standards that most EHRs currently do for data tracking and accounting, thus exacerbating the challenge for other electronic DRSs.

[OCR] request[s] comment on the burdens on covered entities and benefits to individuals associated with also receiving an accounting for disclosures that includes information provided in accordance with the breach notification requirement. With respect to the remainder of public health disclosures (i.e., public health disclosures other than those related to reports of child abuse or neglect), [OCR] request[s] comment on whether there are other categories of public health disclosures that warrant an exception because such disclosures may be of limited interest to individuals and/or because accounting for such disclosures may adversely affect certain population-based public health activities, such as active surveillance programs. (31431)

The EHR Association appreciates the opportunity to comment on this area of the NPRM. In general, we support the exceptions outlined within this section of the NPRM and do not propose any additional exclusions. We do seek clarification, however, on whether these exceptions "may" be disclosed or whether they "cannot" be disclosed, with specific reference to the exclusion for the disclosures to report child abuse or neglect[4].

---

[3] HITECH Act, Section 3000 Definitions. (13) **Qualified Electronic Health Record**. - The term qualified electronic health record' means an electronic record of health-related information on an individual that: (A) includes patient demographic and clinical health information, such as medical history and problem lists; and (B) has the capacity: (i) to provide clinical decision support; (ii) to support physician order entry; (iii) to capture and query information relevant to health care quality; and (iv) to exchange electronic health information with, and integrate such information from other sources.

[4] Section 164.528(a)(i)(1)(B). For public health activities as provided in Section 164.512(b), except disclosures to report child abuse or neglect pursuant to Section 164.512(b)(1)(ii).

[OCR] also request[s] comment on whether the complexity of carving out such public health disclosures would lead to too much confusion among individuals and covered entities. (31431)

The EHR Association supports the exclusions to withhold these disclosures from the accounting requirements.

[OCR requests] comment on whether a shorter 30-day deadline, with a single 30-day extension, will significantly benefit individuals and whether it will place an unreasonable burden on covered entities. (31435)

Coordinating the required information between and among covered entities and business associates could be unworkable in the timeframe identified in the NPRM, as many covered entities have hundreds of business associates. Additionally, the complexity and breadth of the information being requested for collection is greater than has historically been the case, so shortening the timeframe becomes that much more problematic. The EHR Association therefore feels that the initial 30 day deadline will be difficult for organizations to meet and should be reconsidered.

Additionally, we seek clarification on the process for requesting an extension under the regulations identified in this NPRM. This request process is a significant factor in identifying the true burden of the proposed timeframe. We also recommend that the process created to consider extensions not place a significant administrative burden on covered entities, and that any required requests be processed in a timely fashion.

To the extent that the covered entity is able to provide more information, such as a description of the system that is accessing the information, we encourage covered entities to include such information. We recognize that more information than the covered entity's name would be helpful to the individual, but we have concerns about the burden on covered entities if they were to have to describe each internal exchange of information between systems in more detail. In contrast, we believe individuals' interest in such internal exchanges may be limited. We request comment on this issue, particularly the burden of providing identifying information about internal systems and the interests of individuals in learning of such internal exchanges. (31438)

The EHR Association agrees that individuals' interests in these internal exchanges are very limited and could be a source of confusion if included within the accounting.

While [OCR recognizes] that it may be helpful to individuals to learn what information was accessed, we believe that it would be unreasonable to require all covered entities and business associates to modify all of their electronic designated record set systems to collect this information, especially in light of the relatively small number of accounting requests that most covered entities have received to date. [OCR requests comments] on the availability of this information in current access logs, the importance of the information to individuals, and the potential administrative burden of requiring that access reports include a description of what information was accessed. (31438).

The EHR Association is well positioned to provide a response to this question. It is not uncommon for an EHR system to capture within its audit logs a characterization of the type of information accessed – i.e. visit documentation, medication list, etc. – but this information most often does not drill down beyond the category level. As an example, the log would currently indicate that the "medication list" was accessed but would not capture whether it was the medication history or complex dosing schedules that were the final view. The administrative burden becomes a major factor, however, when considering all the electronic systems that contain part of the DRS for any given covered entity. Again, we encourage OCR to consider using the definitions of EHR identified through the HITECH Act to a limited data set included within the audit logs.

The EHR Association recommends another revision based on a similar issue to the above. Currently, most EHR patient-level audit tracking system access reports do not log when a user accesses a "patient list" (e.g., a provider practice schedule or a disease registry report that includes hundreds or even thousands of patients). We are therefore concerned that the proposed regulations assume that such accesses are tracked in a way that can be used to create or contribute to patient-level access reports, and we believe that it would be unreasonable to require that this access be included within the proposed access reports. Ultimately, information on this type of access provides little benefit to the individual and

likely would clutter access reports, even rendering them indecipherable by individuals. This proposal will also place a costly administrative burden on EHR vendors to modify current products to meet these requirements and on providers to purchase significant additional disk space.

[OCR requests] comment on the potential burden to covered entities and potential benefit to individuals of requiring the access report to include address information that indicates where the access occurred. (31438)

The EHR Association agrees with the NPRM's assumption that the address of the access location will rarely be of interest to the requesting individual. EHR systems have the capability to capture the address or "location" of where the access occurred, but the data captured (IP Address, workstation ID, etc.) would likely be of limited value to an individual.

[OCR requests] comment on our proposal to not require covered entities and business associates to include a description of the purpose of access in access reports. (31439)

The EHR Association agrees with and appreciates the proposal to not require covered entities and business associates to include a description of the purpose of access within the access reports. This information is not currently captured and, if required, would likely require additional data entry at the point of the action occurring. This additional data entry would create an undue burden on covered entities and business associates, as well as jeopardize the adoption of EHRs among healthcare providers.

[OCR requests] comment on our assumption that systems do not record information about the purpose of the access and ultimate recipient of the information within audit logs. (31439)

The EHR Association agrees with this assumption. It is uncommon for systems to record the purpose of the access, though purpose can frequently be inferred from the character or sequences of access (e.g., a sequence that signifies a patient admission). In either case, this would be extremely burdensome to covered entities and business associates, so we therefore support its exclusion from the reports.

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. Additionally, the burden of generating access reports will be directly proportionate to the interests of individuals; if few individuals request access reports, then covered entities will rarely need to undertake the burden of generating an access report. We request comment on the above conclusions. (31439)

The EHR Association agrees with the OCR's assumption that aggregating these data into a single access report presents a significant burden to covered entities and business associates, as we've outlined in earlier comments. We disagree, however, with the assumption that the burden to produce an access report is directly proportional to the interest of individuals in receiving this report.

A significant portion of the burden that would be imposed on covered entities and business associates to meet this requirement would be experienced in preparation for the first access report that would be generated. Two examples of the burdens imposed through these proposed requirements would be the purchase of technology capable of producing these reports (financial) and the synching of business practices to collect and aggregate the data from multiple electronic sources (workflow changes, internal costs). We also believe that a sizable number of requests for such reports would cause an additional significant burden, and we encourage OCR to consider the effects that a highly publicized event would have in terms of creating potentially hundreds or thousands of simultaneous requests of an organization.

Given all of these issues, the burden of providing an access report as required by the NPRM is not balanced by the benefit to individuals. In particular, accesses relating to treatment, payment, and health care operations are routine and recurring, and thus are unlikely to be of as much interest to individuals as true disclosures.

[OCR proposes] to provide that machine readable data is digital information stored in a standard format enabling the information to be processed and analyzed by computer. For example, this would include providing the access report in the

format of MS Word or Excel, text, HTML, or text-based PDF, among other formats. We request comment on the ability of covered entities to provide access reports in machine readable or other electronic formats. (31440)

The EHR Association appreciates the opportunity to offer feedback regarding this topic. The likelihood that a covered entity can provide access reports in a machine readable or other electronic format, as defined by the NPRM, is very high. Current audit reports are commonly generated in such human readable electronic formats as PDF and text. To generate the access reports in such electronic formats would be a low administrative burden, recognizing that these formats are not in any way optimized for aggregation across multiple reports or ready computer analysis. Whether creating more structured formats would be burdensome to a covered entity or their business associates depends on standards and formats identified for exchanging the data.

Because covered entities should already be maintaining access logs pursuant to the Security Rule, we believe that it is reasonable to require covered entities to produce access reports, upon request, covering access over the prior three years beginning on the proposed January 1, 2013, and January 1, 2014, compliance dates. We request comment on whether covered entities will be able to generate access reports covering the preceding three years on these compliance dates. (31442)

The HIPAA Security Rule applies to healthcare organizations and provides requirements for organizations' efforts to protect the data that they hold. Conversely, it was never intended to impose a requirement to provide data from a security audit log to patients. The point of the audit requirement is to allow the organization to log information that will facilitate its own security risk management program. The information that is logged is determined by the organization itself, based on its needs.

As implemented and reviewed under current regulation, a security audit log typically contains data primarily on security anomalies and often does not log legitimate accesses, in particular "read" accesses. However, the discussion in the NPRM assumes that "use" data, including data about legitimate, routine "read" accesses, is captured in a security audit log. The NPRM, therefore, imposes a specific standard for data collection in this log, and specifically a type of data <u>not</u> anticipated by the Security Rule.

The NPRM seems to assume that there is a requirement in the Security Rule for organizations to maintain an access log. Our conclusion is that the applicable portions of the Security Rule, especially Section 164.312(b), is much more general than seems to be assumed. The Audit Controls standard requires a covered entity to *"…implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information."*

A CMS resource on the Security Rule states that:

> *Most information systems provide some level of audit controls with a reporting method, such as audit reports. These controls are useful for recording and examining information system activity, especially when determining if a security violation occurred. It is important to point out that the Security Rule does not identify data that must be gathered by the audit controls or how often the audit reports should be reviewed. A covered entity must consider its risk analysis and organizational factors, such as current technical infrastructure, hardware and software security capabilities, to determine reasonable and appropriate audit controls for information systems that contain or use ePHI.*

Regarding the compliance dates, it is reasonable to expect that EHRs capable of producing these reports will be in place by the proposed dates, but it is unreasonable to assume that at the point of the compliancy dates that the covered entity will have three years of data to report in the case of a request for an access report.

[OCR expects] that the additional burden to covered entities will consist of, in response to a request, generating access reports for each electronic designated record set system and aggregating this information into a single electronic access report. The cost to covered entities to prepare an access report would be directly tied to the number of requests. Based on the experience covered entities have reported with requests for accountings of disclosures, we anticipate few requests for

access reports. Therefore we expect the costs to generate access reports will be minimal. We request comment on the number of anticipated access reports, the burden of tracking access to electronic designated record set information, including whether our proposal will have any unintended effects by requiring significant changes to existing systems, and the burden caused by generating an access report. (31444)

As noted above, the NPRM assumes that requests for access reports will be "minimal" based on the limited number of requests for an accounting for disclosures. We recognize that few accounting for disclosures have been requested to date, but caution OCR to consider that should a highly publicized event regarding a patient access report take place, it could quickly prompt thousands of patients to send accounting requests to covered entities across the county.

As we stated earlier, the EHR Association is concerned that using the DRS expands the scope of the access reports beyond what is called for or authorized by the HITECH Act. We also believe that this expansion places an undue burden on covered entities to aggregate the data included within the DRS from EHRs and multiple other electronic systems, which is especially a concern in a hospital context. Again, based on these consequences, we believe OCR should look to the HITECH Act definitions of Electronic Health Record and Qualified Electronic Health Record and limit the accounting requirement to only data "that is created, gathered, managed, and consulted by authorized health care clinicians and staff."

The provision permitting individuals to limit their requests to a time period or person may limit the burden to produce an access report. Yet, modifying a standard report may require additional programming which would increase burden on the covered entity and business associates. We solicit comment on the effects of this provision. (31445)

The EHR Association agrees with the OCR's assumption that modifying these standard reports would require additional programming, thereby increasing the burden on covered entities and business associates. Many EHRs likely provide the ability to sort access reports by both time period and person accessing the report, but they may not have the capability to limit the report to a specific time frame or a specific person. This requirement would either require programming changes or manual modification of the report by the covered entity to meet this requirement. Therefore, we suggest that covered entities be permitted, <u>but not required</u>, to limit access reports based on requester-supplied parameters.

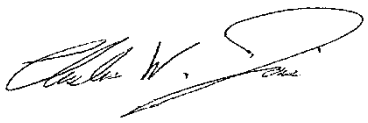
This issue is also related to the concern we have regarding the requirements outlined in this NPRM that assume that it is common practice to collect patient-level user access information when a user accesses something like a provider's practice schedule or a disease registry report containing a limited amount of any patient's information. Again, we believe that it would be unreasonable to require that such types of access be included within the access reports. This type of access provides little benefit to the individual and likely will clutter access reports in such a way as to render them indecipherable by individuals. This requirement will also place an administrative burden on EHR vendors to modify currently certified products to meet these needs at a time when multiple other programs with robust and complex requirements are also rapidly changing the standards to which their products must adhere.

Conclusion

The EHR Association appreciates the opportunity to provide public comments to the Office of Civil Rights on this important Notice of Proposed Rule Making. We look forward to continued dialogue between our Association and its members with the Department in order to help the nation's healthcare professionals and patients both realize the full potential benefits of the HITECH Act.

Sincerely,

Carl Dvorak
Chair, EHR Association
Epic



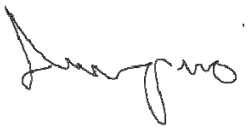
Charles Jarvis
Vice Chair, EHR Association
NextGen Healthcare

HIMSS EHR Association Executive Committee

Greenway Medical Technologies
Justin Barnes

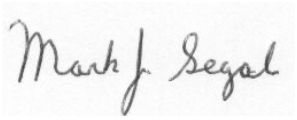
CPSI
Rick W. Reeves

e-MDs
Pamela Chapman



Jacob Reider, MD
Allscripts Healthcare Solutions

Siemens
Michele McGlynn



GE Healthcare IT
Mark Segal

cc: Steve Lieber, HIMSS
Gail Arnett, HIMSS
EHR Association Executive Committee

About HIMSS EHR Association

HIMSS EHR Association is a trade association of Electronic Health Record (EHR) companies that join together to lead the health information technology industry in the accelerated adoption of EHRs in hospital and ambulatory care settings in the US. Representing a substantial portion of the installed EHR systems in the US, the association provides a forum for the EHR community to speak with a unified voice relative to standards development, the EHR certification process, interoperability, performance and quality measures, and other EHR issues as they become subject to increasing government, insurance and provider driven initiatives and requests. Membership is open to HIMSS corporate members with legally formed companies designing, developing and marketing their own commercially available EHRs with installations in the US. The association, comprised of more than 40 member companies, is a partner of the Healthcare Information and Management Systems Society (HIMSS) and operates as an organizational unit within HIMSS. For more information, visit http://www.himssehra.org.