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

RE: Response to “HIPAA Privacy Rule Accounting of Disclosures Under the Health Information Technology for Economic and Clinical Health Act; Proposed Rule,” hereinafter “NPRM” (RIN 0991-AB62).

Dear Secretary Sebelius:

The North Carolina Healthcare Information and Communications Alliance, Inc. (NCHICA) is a nationally-recognized, nonprofit consortium that serves as an open, effective, and neutral forum for health information technology (HIT) and policy initiatives that improve health and care. NCHICA is comprised of over 240 member organizations representing the many sectors of the healthcare industry, including covered entities (CEs), as well as government agencies, business associates (BAs), research organizations, application vendors, consultants, and attorneys.

NCHICA’s role in advancing healthcare technology through the protection of individuals’ privacy and security of individual data with supportive policies has been well established. NCHICA was actively involved in analyzing and providing support to its members regarding compliance with the provisions of the HIPAA Privacy Rule, which became effective in 2003. NCHICA’s comments on this Notice of Proposed Rulemaking (NPRM) are the result of a collaborative effort from NCHICA’s various and diverse member organizations, which have considerable combined expertise in the various aspects of the HIPAA Privacy and Security Rules.

**NCHICA’S COMMENTS ON THE NPRM**

NCHICA commends the Department of Health and Human Services (the Department) on the intent behind these proposed implementing regulations, which are required by the Health Information Technology for Economic and Clinical Health Act (HITECH Act). We appreciate that the NPRM is designed to provide increased transparency to patients by permitting them to access greater information about how their
health care information is used for purposes of treatment, payment and health care operations and supporting an accountable health and care system.

Having said that, it is NCHICA’s view that the proposed modifications to the Accounting of Disclosures, and in particular the NPRM’s addition of a newly created right to an Access Report, goes well beyond HIPAA’s intent and does not materially add to HIPAA’s already strong protections for protected health information (PHI). Our suggestions for clarification to the NPRM follow in the order in which the topics are discussed in the NPRM.

As follows, in response to the Department’s request for comment to the NPRM, NCHICA is providing comment on the following topics:

1. The revised right to an Accounting of Disclosures;

2. The new right to an Access Report
   a. The need for a definition of “access”;
   b. The significant operational and technical burdens the new right to an Access Report would impose;
   c. The difficulties of providing an “understandable” Access Report from currently-available audit or access logs;
   d. The likely increase in complaints to OCR that result in a finding of no violation or cases not eligible for enforcement;
   e. The infringement on privacy interests of employees and the potential misuse of Access Report information;
   f. The exclusion of Patient Safety Work Product and other restrictions on Access Report information;
   g. Issues related to timely response to requests for Access Reports and the effective date of the new right; and


NCHICA believes that clarifications in these areas will better enable CEs and BAs to comply with HIPAA while maximizing the protections afforded to PHI and minimizing unintended consequences that restrict the necessary flow of electronic information.
ACCOUNTING OF DISCLOSURES UNDER REVISED 45 CFR § 164.528(a)

NCHICA appreciates the Department’s efforts to clarify a number of the previous revisions to the Accounting of Disclosures standard. NCHICA commends the Department for modifying the standard from one of exclusion to one where the disclosures for which an accounting is required are explicitly listed. This modification will resolve much of the confusion CEs experienced under the existing Privacy Rule. We further commend the Department for proposing that a CE may provide an individual with an accounting specific to that individual’s request, thereby permitting CEs greater flexibility to narrow the information to be included in the accounting on a specific time period, type of disclosure, or recipient. We further appreciate the changes to 45 CFR 164.528(a)(2) permitting a CE to include in the accounting the name of the entity, instead of the name of the individual recipient of a disclosure, in order to prevent a new HIPAA violation where identification of the entity or person would constitute an impermissible disclosure of PHI about another individual. Further, during our consideration of the NPRM our members raised concerns of personal safety if specific individuals involved in a person’s care or subsequent payment or operations were identified.

We recommend several further clarifications to the standard for accounting to ensure that an Accounting of Disclosures will not be misused in specific situations. For example, we recommend that the Department clarify information about both elder abuse, subject to increased reporting requirements under the Elder Justice Act of the Patient Protection and Affordable Care Act (P-PACA) of 2010, and domestic abuse be treated like information about child abuse and therefore excluded from an accounting. This should include preventing a personal representative from obtaining such information where appropriate and necessary to protect the individual who has been abused. This clarification could be added as a new subsection 45 CFR § 164.528(a)(3)(v), providing that,

RECOMMENDATION:

“The covered entity is not required to provide an accounting to a personal representative, family member, or guardian of an individual where abuse is reasonably suspected or such accounting is otherwise not in the best interest of the individual.”

We agree with the decision to no longer include research disclosures in the accounting for disclosures.
RIGHT TO AN ACCESS REPORT UNDER REVISED 45 CFR § 164.528(b)

OVERVIEW

NCHICA has significant concerns about certain aspects of the Department's creation of a right to an Access Report, at least as that new right is established in the NPRM. NCHICA and its members appreciate and support individual's rights associated with health information and recognize the harm caused by inappropriate access to PHI by authorized and unauthorized users alike. NCHICA believes, however, that the right to an Access Report as detailed in the NPRM is burdensome, not based in statutory authority, and would be largely inadequate to correct the problem of inappropriate or improper access. We implore the Department to reassess the NPRM's Access Report provisions in light of the Security Rule's repeated emphasis on the need for "flexibility of approach" in addressing the requirements of HIPAA. See 45 CFR § 164.306(b)(1) which states that "Covered entities may use any security measures that allow the covered entity to reasonably and appropriately implement the standards and implementation specifications as specified in this subpart." (emphasis added). In contrast to the approach set forth in the Security Rule, where CEs were expressly required to balance factors such as cost, probability and criticality of the risks, and size of the organization in determining how they would comply with the law's requirements, the NPRM offers little to no flexibility on the manner in which a CE would be required to log and produce reports of access in response to an individual's request.

We also are concerned about the Department's assumption that the historical low volume of patient's requests for Accountings of Disclosures likely equates to a future low volume of patient requests for Access Reports. We believe that most patients have not exercised their right to request an accounting in large part due either to: (i) a lack of understanding of the benefits of an accounting; or (ii) the fact that no private right of action exists under HIPAA, so attorneys have not prompted their clients to obtain this information. In contrast, we believe that concerns about unauthorized access to PHI are rising, and that providing such a broad Access Report to individuals will have the unintended consequences of increasing unsubstantiated allegations of improper access, which in turn will subject employees and contractors performing legitimate services to unnecessary identification and scrutiny, and will waste valuable CE and BA resources. For the most part, we do not believe the mere provision to an individual of an Access Report, without the commitment of substantial additional (and currently unfunded) resources to provide interpretation or explanation to the individual about the contents of the report, will target inappropriate access or provide the benefit to individuals that the Department appears to be seeking to address in this section of the NPRM. With this in mind, we implore the
Department to revisit this new right and craft an appropriate mechanism to address the Department’s concerns without the many failings and risks of the proposed approach.

Some concerns raised by our members would be mitigated by more clearly addressing the scope of records and systems to which the new right to an Access Report will apply. For example, there are certain procedures, such as a colonoscopy or an echocardiogram, for which certain patient data is captured during the procedure but not maintained in its entirety for more than a total of two to three weeks. Such data from feeder sources can be best described as “not persistent;” therefore, it is not “maintained” by or for a CE, and accordingly this data traditionally has not been considered to part of the “designated record set” or “designated record set information.”

NCHICA recommends that the definition of the “designated record set” in 45 CFR § 164.501 be clarified so that the “designated record set” specifically excludes records that are “not persistent” and is a subset of all data or information created by or on behalf of a CE. In any event, the “designated record set” should not include source data, such as, but not limited to, slides, films, and tracings that are not transferred to the Electronic Health Record (EHR).

**RECOMMENDATION:**

We request that the Department use clear and consistent terms of phrases in any final rule and not mix similar, but actually distinct, terms like “designated record set” with “designated record set information” or “designated record set system”, which have not been further defined in the NPRM.

We address specific concerns raised by our members about the NPRM’s new right to Access Reports in the following pages.

**THE NEED FOR A DEFINITION OF “ACCESS”**

We believe that CEs require more guidance on what OCR considers “access” for purposes of the “Access Report.” We understand that “access” includes certain “action by the user” of an EHR, such as “create”, “modify”, “access” or “delete.” In some situations, however, what constitutes “access” is not clear. Many times, information that is “viewed” in an EHR is not in fact viewed but, rather, returned in response to a query of appointments, for example. We are concerned that all records returned in response to such a query could be construed as having been accessed and therefore would need to be logged in all such individuals’ records. For instance, entering “John Doe” into the search box of an EMR might return several hundred entries but would only display the demographics necessary to more positively identify the particular “John Doe” being sought. These entries would seem to be of no value to an individual requesting an Access Report and are currently not
logged in many EHRs. To reduce unnecessary information collection and the burden on CEs, we recommend that the Department add a risk-based assessment of access to 45 CFR 164.528(b)(2). A suitable example of regulatory text permitting a risk-based assessment in already found in 45 CFR 164.306(b)(i) - (iv), which includes taking into account factors that include the "probability and criticality of potential risks to electronic protected health information" in a CE’s decision of which security measures to use.

We recommend that the Department add a section like 45 CFR 164.306(b)(2)(i) - (iv) to read as follows:

**RECOMMENDATION:**

45 CFR 164.528(b)(5)

*Flexibility of approach.* In deciding the format and information to use to collect access information, a covered entity must take into account the following factors:

(i) The size, complexity, and capabilities of the covered entity.

(ii) The covered entity’s technical infrastructure, hardware, and software capabilities.

(iii) The costs of access logging and collection measures.

(iv) The benefit of additional access information related to electronic protected health information versus the cost of logging, storing, and translating such access information into an Access Report as required under this subpart.

The definition of access also needs to be refined to exclude data aggregation services and other "back office" operations (e.g. IT operations, system maintenance, and database backups). These activities are performed outside of the clinical applications and the "activity review" records access by the name of the individual whose data is viewed, but rather by the name of the person accessing the data. This lack of tie back to the individual who is the subject of the data makes tracking this type of “access” on a per patient or per individual basis practically impossible with currently available systems.
SIGNIFICANT OPERATIONAL AND TECHNICAL BURDENS ARE CREATED BY GENERATING AN ACCESS REPORT

We are concerned that OCR is under the impression that the generation of an Access Report from the currently available information systems logs or audit trails does not impose significant operational or technical burdens on CEs. Our members have very clearly indicated that the new requirement for an Access Report cannot be met through the push of a button. The “designated record set” exists in a multitude of systems within a single enterprise and in the systems of their BAs. Collection and aggregation of these multiple logs and BAs’ logs and then the further refining of the data to include the appropriate information in a single report in a common format will be time consuming and likely will require substantial manual manipulation. For example, the designated record set of many CEs consists of distinct feeder systems that generate audit logs in differing formats and containing different information. Many systems track according to user IDs instead of user name. Translating these differing formats and information into a single comprehensible Access Report will place a significant burden on many CEs and require upgrades to existing systems that will need to be provided by their vendors in most cases. As noted below, we believe most individuals would not understand or be able to interpret accurately a report based on the audit logs generated by information systems today.

The NPRM’s new Access Report requirements would impose tremendous technical burdens on CEs and BAs. These burdens include the generation of millions of log records to be stored, associated storage space, personnel to manage this system, query capability in multiple systems for a large volume of data to extract requested data for the reports, and ultimately having the ability to correlate the data to the audit logs in a meaningful, accurate, and manageable way.

One example from within our membership is that the estimated resources and costs associated with one team developing a product to comply with the NPRM and its Access Report as 10,000 hours in development time, plus the cost of management, quality assurance, testing, software and hardware-related costs, installation, and implementation, which amounts to millions of dollars. Health information teams at CEs are currently upgrading to ICD-10 and implementing the requirements for “meaningful use”. These are significant enterprise endeavors, taking substantial resources, time, and commitment as teams work across disparate systems.

RECOMMENDATION:

We recommend that OCR consider minimizing the unintended consequences and burdens that likely will arise from the NPRM by realigning the proposal for the contents of an Access Report to conform to the requirements of “meaningful use” and thereby avoid creating an additional burden on covered entities.
Some of our hospital members reported a total volume of audit logs in the range of 400 million to 3.2 billion records annually for a partial list of their designated record sets. One member reported a partial access listing averaged 170 accesses for outpatient visits and over 1800 accesses for a typical 6-day inpatient stay. These examples are an underestimate of those required under the NPRM’s Access Report. Maintaining logs containing the level of detail required by the NPRM will result in considerable storage costs. If the overall scope of an Access Report in the final rule is restricted, then some of the overhead and costs could be reduced.

In addition to the changes that need to be made on a systems basis, CEs will need to revise their BA agreements to reflect these new requirements. For most CEs, this will be a time-consuming and costly process of drafting, negotiating, and executing agreements with numerous vendors. We recommend that OCR consolidate any changes needed to be made to BA agreements under this NPRM with other currently outstanding HITECH changes to the Privacy and Security Rule so that the costs and resources associated with changing the BA agreements can be reduced.

In summary, our members have expressed significant concerns because the logging capabilities of currently available EHRs are less robust and standardized than the Department assumes. A significant shortfall of the NPRM is the Department’s overly optimistic estimate of current access log capabilities, and that access information logged in the current state likely will address patients’ expectations of receiving meaningful information about who accessed their PHI and why.

**INDIVIDUALS WILL NOT UNDERSTAND THE LOGS THAT ARE CURRENTLY GENERATED BY EHRs, AND TRANSLATING OR RENDERING THESE LOGS “UNDERSTANDBALE” WILL REQUIRE SUBSTANTIAL TIME, STAFF EFFORT, AND RESOURCES**

As we have previously stated, the information generated by currently available audit controls and access logs is not typically in a format that a person unfamiliar with information technology would understand. Converting the logged information into a usable and understandable “Access Report” as currently described in the NPRM will take significant time, effort, and resources. In addition, once produced, the Access Reports are likely to raise many more questions than the answers they provide. Patients likely will not understand the logs and will have numerous questions about information contained in them; the need to respond to this increase in patient questions will likely create significant customer services concerns for covered entities. We believe without question that the typical individual is unaware of the number of employees that routinely access that individual’s information in the course of treatment, payment, and health care operations, let alone other legitimate uses or disclosures of PHI.
CONCERNS ABOUT THE LIKELY INCREASE IN UNSUSTANTIATED COMPLAINTS TO OCR

In addition to our concerns about the burden on CEs and lack of benefit to patients, our members are concerned that Access Reports will result in a substantial increase in complaints alleging violations of the Privacy and Security Rules, many of which may be founded on misinformation or mistaken impressions about the number of individuals who legitimately and typically have access to ePHI.

We recognize that there is certain information that individuals would expect or want to see in an Access Report, but there is also other access information that is generated in the course of health care treatment, payment, and operations that would not be of interest to most, if not all, individuals. For example, a patient might be interested in whether a specific person has accessed his or her information, but not interested in the fact that many employees legitimately accessed the patient's information to perform their job duties. However, due to increased attention being paid in the media to inappropriate access of PHI and other personal information, we are concerned that individuals may be reluctant to limit their Access Report requests to the specific individuals or time frames about which they are truly concerned, believing that a broader report will enable them to detect whether there has been any inappropriate access to their PHI. We do not believe that the Access Reports, as currently outlined in the NPRM, will permit individuals to easily make this determination.

Moreover, patients generally do not understand that multiple users legitimately need to access their records, including accessing records multiple times, in the course of their job functions. Nor do individuals understand that for many legitimate and necessary purposes, CEs share information with BAs. Individual education on the meaning of the report content will require significant staff resources, yet the failure to provide such education most likely will result in a substantial increase in patient complaints to both CEs and OCR. OCR will have to investigate such complaints, which will require additional staff, time and resources. Unfortunately, such complaints will shift resources and staff away from other investigations. The end result is likely the inefficient use or waste of OCR's and CEs' resources when individuals file unsubstantiated complaints based on such individual’s misunderstanding of the information contained in an Access Report.

PRIVACY AND SAFETY INTERESTS OF EMPLOYEES AND POTENTIAL MISUSE OF ACCESS REPORT INFORMATION

Our members have expressed concerns about the interests of the persons whose names will be listed in Access Reports. First, we have serious concerns that the Access Report as proposed may jeopardize the privacy interests of CE employees. Second, our members have raised concerns about how to protect the safety of employees or staff who work with particular patient populations. Third, we are concerned that in some instances
Access Reports will be requested solely to investigate potential complaints or for the purpose of pursuing claims in litigation. We believe these concerns all require modification of the Access Report provisions NPRM to appropriately protect employees.

We have concerns that the Access Report as described by the NPRM will provide significant information about employees of covered entities, thereby unnecessarily subjecting such employees to potential litigation and harassment by patients and counsel for patients. These Access Reports will give patients access to staff names and permit intrusive behavior. The NPRM places no controls on how Access Reports can be used by individuals; accordingly, we do not see how CEs will be able to prevent various types of behavior adverse to CE staff, ranging from harassment and fishing expeditions which may lead to litigation.

When treating certain patient populations, there is a heightened need for instituting protections for treating practitioners and staff. For example, many of our members have indicated that full names of practitioners and staff typically are not available on name tags, directories, or in other locations in which certain patient populations, including mental health and emergency department patients, are treated. The risk of patients potentially harassing or causing harm to these practitioners and staff, already has been determined to be high enough risk to outweigh any benefit to patients in identifying the full names of the employees. For the same reasons, many working with these populations have unlisted telephone numbers or other contact information. The Access Report requirements of the NPRM would remove these protections from individuals who provide these important services.

In addition, the proposed requirement that Access Reports name individual employees who accessed information likely will increase the number of patient concerns about access in other common workforce situations. These include situations where a patient’s neighbor is an employee or practitioner on a care team or where employees are patients. In these situations, we are concerned that an Access Report will permit individuals to subject many employees or practitioners who are simply performing their usual job functions to additional employment scrutiny and investigation.

We believe that a request for an Access Report is most likely to be made where an individual either has received a breach notification or some other indication that his or her information has been inappropriately accessed. In general, it is believed that patients are not interested in who created, modified, accessed, printed or deleted their information. We also believe that Access Reports may be requested frequently in an effort to develop private claims, complaints, or lawsuits based on allegations of wrongful access (or improper trade practices). Our members are concerned that under the NPRM, individuals will have a list of all employees who accessed information which they may use for any purpose, legitimate or otherwise. Plaintiffs’ counsel and defense counsel likely will request
these types of reports, and each employee named in an Access Report in their role as a member of the CE’s workforce will be vulnerable to being contacted in litigation.

We are also concerned that personal concerns of employees regarding access logs may cause them to avoid accessing a record due to a fear of being targeted by a "difficult patient." This unintended consequence could lead to medical errors and worse outcomes.

**Exclusion of Patient Safety Work Product and Other Limitations on Access Report Information in the NPRM**

NCHICA commends the Department on recognizing the importance of protecting Patient Safety Work Product ("PSWP") as defined by the Patient Safety and Quality Improvement Act of 2005 and associated regulations in 45 CFR § 164.528(c), and otherwise providing some limitation on Access Report information in the NPRM. We believe that it is both necessary and appropriate to protect PSWP, including its exclusion from Access Reports. The feasibility of excluding any particular source of information or information system from the Access Report, as broadly described and implemented in this NPRM, however, seems difficult, if not impossible.

**Issues Related to Response Time and Effective Date**

We have significant concerns about the ability of any CE to generate the type of report envisioned and seemingly required by this NPRM within thirty (30) days of receiving a request for such an Access Report. We believe that a compliant response, including the time to gather, consolidate and create a single report in a complex environment and potentially involving BAs, will take on average 45 to 60 days.

With this in mind, we suggest that 45 CFR § 164.528(b)(3)(i) be revised to read: “

**Recommendation:**

45 CFR § 164.528(b)(3)(i)

"The covered entity must act on the individual's request for an Access Report no later than 60 days after receipt of such a request."
RECOMMENDATION:

To the extent that the Department retains the newly created right to an Access Report, we recommend that the Department delay the effective date of any right to an Access Report until the widespread implementation of EHR systems that are compliant with the staged requirements of Meaningful Use. Such a delay would permit currently available EHR systems to be modified to address compliance with this newly created right and will enable implementation of the right in a manner that better serves both individuals and CEs.

CONFORMING CHANGES TO NOTICE OF PRIVACY PRACTICES UNDER REVISED 45 CFR § 164.520

The NPRM obligates CEs to amend further their Notice of Privacy Practices (NPP) to conform to changes to the Accounting of Disclosures standard and to address individual's new right to an Access Report. NCHICA supports the need for clear communication regarding individual rights in health information privacy and security. Given that additional changes to NPPs have been proposed by the Department but have not yet been finalized, NCHICA recommends that the Department set a reasonable effective date for CEs to revise their NPPs to address all necessary changes to be made arising from this NPRM and the NPRMs published in 2009 and 2010 associated with breach notification and other changes to the Privacy and Security Rules specified in the HITECH Act.

As we have stated in comments we filed with the Department regarding the July 14, 2010 HITECH Act NPRM, the costs and time associated with revising and redistributing the NPP of a CE in either paper or poster form can be significant whether the CE is a health plan or a provider, although admittedly the scale may differ. In previous NPP revisions, our members have incurred significant costs and expenses per draft revision that the Department identifies in the NPRM's Regulatory Flexibility Analysis, and therefore we believe that the costs of these revisions will substantially exceed the $20.2 million figure estimated. Not only does the NPP revision process require staff time and effort in both creation and distribution of the NPP, it also frequently leads to additional costs, such as legal review, publication, formatting, and other professional services.

RECOMMENDATION:

Given the process involved in revising NPPs, NCHICA requests that the Department consider a process that will avoid the time, effort, and cost of revising NPPs multiple times.
SUMMARY

NCHICA appreciates that the Department issued this NPRM to implement the provisions on accounting of disclosures set forth in the HITECH Act. While NCHICA agrees that provisions of the Privacy and Security Rules must be revised to achieve the goals of the HITECH Act, NCHICA urges the Department to revise the rules on Access Reports contained in this NPRM to avoid unintended consequences, including confusing individuals by providing lengthy reports containing a large quantity of irrelevant information and overburdening CEs and their BAs beyond the requirements of law.

The member organizations of NCHICA include CEs and BAs, research entities, and aggregators of health data, as well as other entities that support them every day. Our member organizations recognize that inappropriate access to PHI is a significant concern and we all are committed to the goal of an accountable health and care system that protects individual privacy and engenders consumer confidence. However, NCHICA is very concerned that the Department’s creation of a new right to an Access Report, not based in any existing statutory or regulatory authority, likely will have unintended and unanticipated consequences that may negatively affect treatment, payment, and health care operations and other necessary activities of CEs and their BAs.

NCHICA recommends that the Department reconsider whether the new right to Access Reports is in the best interests of patients, CEs and BAs alike and, should the Department determine to retain this new right, NCHICA believes it is imperative that the Department revise these proposed rules as noted herein before issuing final regulations.

Respectfully submitted,

W. Holt Anderson
Executive Director

John M. Jenkins
President

William D. Mattern, MD
Chairman of the Board

North Carolina Healthcare Information and Communications Alliance, Inc.
PO Box 13048, Research Triangle Park, NC 27709-3048
(919) 558-9258  www.nchica.org