AMIA

INFORMATICS PROFESSIONALS. LEADING THE WAY.

July 30, 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 509 F
200 Independence Avenue, SW
Washington, DC 20201

45 CFR Part 164
RIN 0991-AB62

HIPAA Privacy Rule Accounting of Disclosures Under the Health Information Technology for Economic and Clinical Health Act (HITECH)

Notice of Proposed Rulemaking (NPRM)

Dear Secretary Sebelius:

On behalf of the American Medical Informatics Association (AMIA), I am pleased to submit these comments in response to the above-referenced proposed rule. We thank the Department of Health and Human Services (the Department) and the Office for Civil Rights (OCR) for issuing this proposed rule, which modifies the HIPAA Privacy Rule's standard for accounting of disclosures as called for by Section 13405(c) of the HITECH Act (Pub. L. 111-5). In providing input, we will respond to the requests for specific comment included in the NPRM, but we will begin by discussing the basic assumptions and framework of the proposed rule.

General Comments: The NPRM's Revision of §164.528 (Accounting of Disclosures of Protected Health Information)

The NPRM serves to revise the obligation of Covered Entities (CEs) to provide an accounting of disclosures of an individual's protected health information (PHI) as directed by Congress in HITECH, but then goes further in proposing to require CEs and their Business Associates (BAs) to provide an "access report" that indicates who has accessed an individual's PHI, a requirement not required by the legislation which HHS proposes to create using its "more general authority under HIPAA".

In regard to the NPRM's revision of the current Accounting of Disclosures requirements, [at proposed §164.528(a)], AMIA largely applauds the changes proposed by the Department: "We propose to change the scope of information subject to the accounting to the information about an individual in a designated record set, to explicitly include business associates in the language of the standard, to change the accounting period from six years to three years, and to list the types of disclosures that are subject to the accounting (rather than listing the types of disclosures that are exempt from the accounting)." The NPRM specifically proposes to exempt from the accounting requirement disclosures made for research purposes under §164.512(i), which includes research projects in which an IRB or Privacy Board has exercised its authority to waive individual authorization, activities preparatory to research, and the like, an action consistent with recommendations made by the Secretary Advisory Committee for Human Research Protections (SACHRP) and a recent Institute of Medicine (IOM) report. We believe that exempting such non-interventional, information-based research from the accounting requirement will represent a first small step toward lessening the heavy administrative burden that has been placed on health services and other research, (even while achieving little in terms of actually protecting privacy). AMIA is similarly supportive of the proposal to exempt from the accounting requirement disclosures that are required by law or made for health oversight purposes.

By contrast to the apparent balancing of benefit and burden that the Department took in revising the accounting of disclosures requirement, we believe that the proposed new right to an "access report" [at §164.528(b)] reflects both an inaccurate and unreasonable interpretation of the HIPAA Security Rule and a dramatic misjudgment of the capabilities of the applicable technology in the healthcare industry. We believe that this report will provide little reasonable benefit to individuals, that the primary interests identified for individuals can be served in much narrower ways, and that the rule – if applied as proposed – would require significant new technology efforts and expenditures from virtually all companies in the health care industry, with substantial ongoing burden.

In this NPRM, HHS makes assumptions based on a not previously articulated interpretation of the HIPAA Security Rule at §164.308(a)(1)(ii)(D) and §164.312(b), evidently viewing these sections as requiring more than simply the recording and examination of information system activity, "such as" through audit logs and access reports. HHS flatly assumes that all CEs and BAs, large and small, are today generating detailed, integrated and comprehensive audit trails of individual access to electronic health information systems. This assumption appears to be the basis for the Agency's belief that implementing a new HIPAA right for individuals to know who has viewed their PHI will be an easy and almost cost-free exercise. In fact, current EHR systems were not developed with this requirement in mind, and most would be unable to support this new requirement without modification. While it may be possible for internal EHR systems to produce access reports upon request, it would be very difficult and time consuming to gather the same information from BAs.

The NPRM further assumes that by limiting the access report requirement to the designated record set (DRS) the requirement will represent a minimal burden for covered entities. However, we see two problems with this assumption. First, the NPRM refers to "designated record set," "designated record set information," and "designated record set systems" which seems hopelessly to muddle an already extraordinarily complex definition, (a level of complexity, we might add, that is not lessened by the NPRM's almost willful misreading of the definition at §164.501 as suggesting that the DRS is a "set of records" that is *always* used to make decisions about individuals, rather than a set of records maintained, collected, used or disseminated by a CE **or** used to make decisions about individuals). Second, we are troubled by the Department's assertion, "We also note that a covered entity will usually have electronic designated record set information in multiple systems which each maintain separate access logs. **Our expectation is that data from each access log will be gathered and aggregated to generate a single access report (including data from business associates' systems** [emphasis added]." To quote one hospital CMIO, "my hospital uses 48 major IT systems and 116 smaller ones, and another CMIO told me that his hospital has 353 major systems and a total of 840 different systems." Simply, the idea that generation of a single access report will require only an "EASY Button" is, we believe, inconsistent with reality. (To advance the argument further, far from being a useful limiting characteristic of health information, the very notion of a "designated record set" may be an increasingly outmoded concept in the context of a fluid, comprehensive, interoperable electronic data environment.)

As the NPRM correctly notes, Section 13405(c) of HITECH directs the Secretary "to balance the burden imposed on covered entities with the interests of individuals to know about the **disclosure** [emphasis added] of their protected health information." We do not disagree that some number of individuals have an interest in learning about routine disclosures that may be made outside of the health care organization to which they have entrusted their care (or payment for their care), disclosures captured under the rubric of "treatment, payment and health care operations." However, we disagree that the new access report requirement offers a "significant benefit… in that it provides individuals an opportunity to **learn of access by members of the covered entity's workforce** [emphasis added]", a disagreement further reinforced by the Department's assertion that "we anticipate few requests for access reports"; simply, we are hard-pressed to understand how an unprecedented regulatory burden can offer a "significant benefit" if few individuals are likely to avail themselves of the right.

In fact, in our judgment few individuals would find any benefit at all without a good deal of education about the use and disclosure of information in the modern healthcare environment. To quote one of our members: "Providing a list of who saw your record will *not* in any way -- hamper those stealing entire data banks of medical records; help you figure out who the 14th phlebotomist was who came to your room and looked funny; help you understand why 60% of the people who accessed your records were associated with insurance institutions and financial processes; help you explain why six nurses reviewed your medication list on Thursday morning because some meds were missing from the cart, some had unreadable barcodes, some were mis-specified because the drop down menu on the CPOE screen was confusing help you understand that there are three handoffs among residents and three handoffs among nurses, plus there are two rounding teams that will review your records if you are very fortunate."

Another AMIA member voices the problem as a concern: "On a typical day, there could be many legitimate accesses, some by students and trainees, which would require a large amount of education and communication to the end users once a question arises. I am afraid that forcing institutions to try to track every access will cause institutions to stop doing things that are hard to record; the worst case scenario is that quality will decrease and patients will be harmed."

Beyond questions of the benefit to individuals and the burden on covered entities and business associates of the proposed access report requirement, AMIA is concerned about the question of where an individual's rights to know about accesses to their information, (all of which accesses are legitimate unless there is some specific reason to believe otherwise,) run up against the rights of CE and BA workforce members to pursue their jobs under agreed-upon conditions, including a presumed right to safety and some measure of privacy within the workplace. §164.528(b)(1)(C) requires that an access report include "Name of natural person, if available" – we are concerned that such a disclosure of an individual's name outside the workplace is not so different from an unauthorized disclosure of PHI, a disclosure to which the individual has not consented. If the patient's actual question is, "Did my ex-girlfriend, who was not involved in my care, look at my record?" would that question not be better understood as a legitimate query of a CE's compliance with the Privacy and Security Rules rather than as implying a broad "right" to information about the identities of members of the healthcare workforce?

Simply, we are concerned with the safety and privacy of the individuals who are accessing health data in the conduct of their jobs, and we believe the Department's recommendation that the identity of every individual who has accessed a record be disclosed to any individual upon request is ill-advised.

To summarize our general comments, AMIA very much supports the reasonable modifications to the accounting of disclosures proposed in the NPRM, but we believe that the proposed access report requirement would represent a fundamental and unnecessary change to a regulatory regimen that has been in place for nearly 10 years. Especially in light of the extraordinarily limited input the Department has relied upon – a single RFI in 2010 to which HHS received "approximately" 170 responses – AMIA suggests that HHS should re-evaluate this proposal for a HIPAA access report right [at §164.528(b)], and we encourage the Department to withdraw the access report provision of the proposed rule

Responses to some specific queries in the NPRM

- Will it be possible for CEs 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?

  Most EHR systems store the data elements at the application or database level. It is not in a form that would provide a readable report to the patient. Several systems may be subject to the request and therefore would need to be matched together in one report for the patient. Tracking and storing disclosures for treatment, payment and operations would require significant data storage and analysis before it can be placed in a readable report. The full impact and cost of storage of such large amounts of data will be significant and include technical and human resources. EMRs can capture each access with split-second accuracy. Many of the separate entries are made within one or two seconds of each other. In fact, when a care-giver obtains access to the electronic health record, s/he typically reviews a number of separate parts of the record in rapid succession. Thus, when a care-giver spends “a few minutes” on the computer looking at a patient’s record, s/he may generate anywhere from 3 to 20 separate rows in the audit log, and, correspondingly, 3 to 20 separate entries in the access report.

While over-reporting accesses by a single caregiver, an audit trail may not capture all user access points. For example, where a staff member looks at a patient schedule on which the patient’s name may be located or generate a list on which the patient’s name is located would not generally create an audit log of this access. Therefore, the audit trails, depending up on what HHS is expecting, may not be complete due to system limitations.

Further, we note that without a greater understanding of the technology that will ultimately be in place, there is no way fully to understand the impact cost this requirement will have on CEs. The cost estimate for this new requirement seems to be unreasonably low, and does not take into account the cost of new software, the manual processes that likely will be needed to cover gaps in the technology, and the training requirements for staff.

The NPRM appears to indicate that the meaning of “access” under proposed 164.528(b) may be more expansive than the definition of access found at 164.304 – “the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource” – but then fails to provide a new definition of “access”. Absent a clear and specific definition, our members raise a number of questions that would require clarification. For instance, does “access” include seeing a patient on a list of scheduled patients for the day? Or, if I run an SQL query that analyzes a patient's record among many others, did I access it? (If so, each record in a typical Enterprise Data Warehouse (EDW) will have thousands of accesses week.) Is seeing a patient name as one of a list of potential matches while I am trying to look up a different patient "access"? Institutions log when one person is looking at details of one patient, usually. They do not typically log every patient displayed in every list or every EDW query. If an EDW generates an operational report in excel format, do we need to track everyone who looked at the report (in excel)? If a patient is discussed in tumor board, and data are displayed for discussion, does a CE need to track every person in the room (they cannot do that automatically). If a patient is discussed at a conference, does the CE need to record attendance? What about medical rounds? If a guest expert is doing rounds with the team, how does the CE record that?

- How difficult will it be for a CE to aggregate data from distinct systems that maintain separate access logs into a single access report? Will the burden of generating access reports be proportionate to the interests of individuals? Do individuals have an interest in learning who has accessed their PHI?

  Data exists beyond the EHR in all cases. Moreover, in a decentralized model, you could have dozens of applications that may not “talk” to each other. Today, each patient request would need to be customized for that individual. There are several data mapping requirements and formatting that are required to obtain a full access report across multiple applications. EHR systems are ‘automated’ in collecting information and storing it as part of an application. However, a significant amount of manual effort and expertise would be required to develop an access report. The data would need to be interpreted for accuracy, as would the report itself. For example, one of our members indicates that one EHR application has a "tracking list" that contains a list of the entire current Emergency Department (ED) census, showing names and locations of ALL patients currently in the ED. It is accessible to all ED personnel, and it is a very useful and often-used tool. The issue arises because of how access to the tracking list is recorded in the audit logs. If an ED nurse named Jean Jones clicks on the tracking list to find out the location of patient Sue Smith, the audit log produces a line showing that Jean Jones gained access to the medical record for **every single patient in the ED**. Thus, in Sue Smith's audit log there will be an entry showing "tracking list" access by Jean Jones, but also the same entry (at exactly the same time) will be generated for all current ED patients. In fact, it is likely that if Sue Smith stays in the ED for any length of time, she will have *many* (anywhere from 10 to 100) rows that seem to show tracking list access to her record by various ED personnel, when, in fact, there is NO way to tell whether the personnel obtaining access to the tracking list looked at any information related to Sue Smith.

If an ED care-giver actually wants to provide care to a specific ED patient and to note such care in the patient's record, then the care-giver will specifically establish a role in that patient's medical record, and from that point on, all access by that care-giver in the patient's record will be accurately and appropriately recorded in the audit log. But all access via the "tracking list" is non-patient specific, because the list is simply that – a list of many different patients. The person accessing the list can look information about one patient or about three patients or about all the patients in the ED, and there is no way to know which patient's or patients' information was viewed.

Put simply, this EHR application works well operationally for ED workflow. Unfortunately, however, the workflow and the way access to the "tracking list" is captured in the audit log do *not* provide accurate information about who obtained access to a specific ED patient's information.

One hospital CMIO says, "We have over 200 distinct information systems including dozens of clinical information systems. There is not a standard format for access logs. Again, our experience is that only 1 out of every 50,000 to 100,000 patients ever requests access to information about who accessed their PHI."

Given the burden of providing these reports and answering the subsequent questions about why is "person X" looking at my record, many institutions may try to reduce the number of individuals with access to records to those who are easier to explain. As a result, many students may be denied access. For example, an informatics student who is working on a decision-support rotation needs to access the record in order to build the decision tree model. Organizations may simply end such access to avoid having patients someday complain that they cannot understand why a science graduate student has been looking at their record.

In short, we do not believe that the cost of implementation is proportionate to the gain for an individual because it is difficult for an individual to understand the complexity of patient care and the multiple ways in which patient data are legitimately used in a healthcare environment.

- Do current systems record information about the purpose of the access and ultimate recipient of the information within audit logs?

  For individual record access, a certified EHR may record the purpose of the access and the ultimate recipient of the information within the audit log. However, many systems do not record purpose because they do not 'automatically' know. And for data transmission such as to business associates or HIEs, the originating source would not know the ultimate recipient of the information. Such an exchange is not necessarily logged at the patient level, but most likely a scheduled batch job to transfer data which is logged as an event (i.e., transfer of data), but not logged as a part of the security log that would be normally used to ascertain who had accessed a particular patient's data. So, the burden of including that information would be great, and the only information somewhat readily available would be a listing of all routine transfers of data between systems, rather than those internal exchanges of information that included the patient's data specifically.

  A typical clinical encounter has several people looking at PHI. If access logs do not continue to be automatically generated (i.e., if they require manual input as to why a record is being accessed), the burden to people looking at PHI will be significant (tens of thousands of extra "clicks"/data entry point per provider per year for a typical practice).

  In terms of the ultimate recipient, again, it is important to recognize that audit logs are usually automatically generated and therefore not able to record whether the ultimate recipient is someone other than the person initially viewing the data.

- The NPRM does not require CEs and BAs to include a description of the purpose of access in access reports. Are individuals interested in learning where their information was accessed, and who accessed that information? What additional burdens might CEs have to take on for the access report to include address information that indicates where the access occurred?

  In order to track both who and why record access occurred, CEs would need to implement a different type of authentication system, one that can associate an identity with the organization to which the identity belongs, that is, a federated identity. In terms of location of access, this would be very difficult, and would require a network-based identity or other mechanism that would be geographically based.

  The key to efficient audit logs is automatic entry of the information in the log. It is unclear why a patient would be interested in learning where their information was accessed. (Does "where" refer to geographic location? Providers who travel often access patients' records all over the country and even throughout the world, but it is not clear why a patient would be concerned that a physician with valid access looked at their PHI in Cleveland or San Francisco.) If manual data entry were required to determine where the access occurred, the burden would be significant.

- How difficult would it be for CEs and BAs to modify their electronic designated record set systems so that access reports could include a description of what information was accessed?

This audit functionality would have to depend on the EHR vendor, and also on the granularity desired in the description. For example, it is one thing to know the encounters that were viewed, if a lab result was opened, etc. However, knowing if a particular vital sign was viewed, specific allergy was seen, or particular family history was observed is a much more detailed and presumably more complicated description.

In many institutions current audit trails provide some level of detail regarding what information or at least what page in the electronic medical record that the user accessed. However, the difficulty of modifying existing electronic designated record set systems so that there was a more detailed description of what information was access will be significant.

- How much burden would be placed on CEs if they were to have to describe each internal exchange of information between systems in more detail? How difficult is it to provide identifying information about internal systems? What are the interests of individuals in learning of such internal exchanges?

CEs should have a detailed knowledge about their internal data exchange. However, there is an enormous difference between processes for and principles of internal data exchange and a system that tracks each specific exchange of healthcare information relating to specific individuals between organizational systems. The NPRM presupposes that log information is gathered in a certain way: that every action is tied to a patient's data. That is not the case, nor is it a requirement under the HIPAA Security Rule as a mechanism to ensure access rights are being appropriately utilized.

As noted by one of our members, "The best description from one of our developers was that of front office / back office. For the front office work of providing patient care, all access is tied to a patient's data. For the back office work of ensuring that information technology systems operate properly and troubleshooting problems (and overall quality or operational improvement at a systems level), the logs capture the actions of the user, but those actions are not always specific to a particular patient's data, so those logs are not designed to tie the action to individual patient's access logs (unless the user is specifically looking up one individual patient). The information could be backed into, through great amounts of rework and effort, but it is not readily available and the burden to generate it would be unreasonable."

Even in a healthcare system with a "single" dominant electronic health record, there can be dozens of interconnected clinical information systems. There would probably be significant burden to describe each internal exchange of information among systems, depending on the detail required. It is impossible to assess how difficult it would be to provide identifying information about internal systems without knowing the identifying information needed. Also, much of this information may be confusing for patients to understand and the specific interests of the individuals in learning of such internal exchanges are unclear. (For example, why would a patient be interested in admission, discharge, or transfer information about them being sent throughout the hospital during an inpatient stay?) Understanding the internal exchanges typically also requires some understanding of how hospitals and healthcare systems work, which may be beyond many patients.

Additionally, we are uncertain as to the value of such detail to an individual. To illustrate by analogy, when we eat a meal at a restaurant the calories, fat, sugar contents may be useful to know, but not how many hands touch the food before it goes into the oven.

- What additional burdens would CEs face if they were required to provide accountings in a machine readable or other electronic format?

  This would depend on the capability of the EHR vendor. Some more robust electronic health record systems could already output audit logs in a machine readable electronic format, although there are not standards for this. Processes that are not currently in place would need to be developed so that such information could be provided in a machine readable or other electronic format. This may require purchasing equipment and spending time and resources on creating such processes.

- How many access report requests might a CE expect to receive in a given year? What will be the cost generating access reports, and maintaining systems that make it possible to generate them? Would the access report requirement necessitate significant changes to existing systems, or could it have any other unintended effects?

  AMIA anticipates that most CEs will receive few (and possibly near-zero) access report requests in any given year – which is why we are deeply concerned that the cost of maintaining systems that make it possible to generate such access reports is entirely out of balance in regard to the potential for benefit to individuals. Access report information would not generally be useful to patients. It might be requested in particular by those contemplating legal action, depending on the basis for the complaint. Perhaps, there might be other requests from persons contesting billing, government agencies looking for fraud in billing, or insurance companies looking to verify billing, although it is not clear how information regarding access to patient data would be useful in these cases.

  We believe that the Department has underestimated the cost of compliance by hundreds of millions of dollars, as hospitals, for instance, will spend hundreds of thousands to many millions to put into place systems that can meaningfully aggregate accesses and internal disclosures across multiple services, departments, business units, etc. In terms of unintended effects, aside from having healthcare providers devote finite resources to collecting and displaying information rather than providing care, we would anticipate a diminution of trust in the healthcare system and possibly an increase in complaints, and even lawsuits.

- Will permitting individuals to limit their requests to a time period or person limit the burden to produce an access report or would modifying a standard report require additional programming which would increase burden on the CEs and BAs?

  While we think the Department is correct in hypothesizing that many individuals would want an access report to answer a specific question – *did my ex-girlfriend who works at your institution look at my record?* – the difficulty is that the audit system, rather than being constructed to audit or check on or verify the appropriateness of accesses, will instead need to be programmed to generate meaningless, endlessly detailed lists of individuals. In the end, CEs will have to build or modify or implement such systems even if, as is likely, they NEVER receive a request for a complete listing of accesses over a three-year period.

  In terms of current experience, one institution reports that the overall rate of access report requests is somewhere on the order of 1 per 50,000 to 1 per 100,000 patients. They indicate that pulling together the disclosures report from different systems takes several hours of work by their Privacy Officer and their team at an estimated cost of several hundred dollars. If requests for access reports were to become common, we anticipate that these costs would increase considerably.

- How difficult will it be for CEs to respond to requests for accountings of disclosures in 30 days, rather than 60 days?

  The shorter timeline would be very difficult to meet for many CEs to meet, given the various sources from which disclosure information must be gathered. However, if robust and well integrated electronic health record systems are implemented reporting in 30 days rather than 60 days would not be difficult. That said, we believe the timeframe for response should be left at 60 days since, if the NPRM moves forward without change, Covered Entities will be required to gather data from Business Associates. This will allow both the Covered Entity and the Business Associate the time to be able to comply with the accounting (and far more complicated) access report requirements.

- Is it a significant burden on CEs and BAs to maintain information on six years of disclosures, rather than three years?

  Yes. Many healthcare systems have not had robust (or any) electronic health records in place for very long, so the burden would be significant. Furthermore, the availability of information more than three years old is of little value to the individuals.

- Should the Department exempt from the accounting requirements certain categories of disclosures that are currently subject to the accounting, such as disclosures about victims of abuse, neglect, or domestic violence under § 164.512(c); disclosures for health oversight activities under § 164.512(d); disclosures for research purposes under § 164.512(i);1 disclosures about decedents to coroners and medical examiners, funeral directors, and for cadaveric organ, eye, or tissue donation purposes under § 164.512(g) and (h); disclosures for protective services for the President and others under § 164.512(k)(3); and most disclosures that are required by law (including disclosures to the Secretary to enforce the HIPAA Administrative Simplification Rules)?

AMIA strongly supports these changes.

- What is the value of the current accounting for research disclosures to individuals who have used or might in the future request such an accounting? Are there alternative ways HHS could provide the individual with information about the CE's research disclosures, such as the IOM's recommendation for a list of all IRB/Privacy Board approved studies? Could other types of documentation about the research be provided to the individual in a manner that is potentially less burdensome on CEs but still sufficiently valuable to individuals?

  Currently, disclosures of PHI made for research purposes are exempted from the accounting requirement if the individual authorized the disclosure, or if the information was contained in a limited data set as defined at 164.514(e). Again, we are very pleased that the NPRM proposes to also exempt research activities undertaken per 164.512(i). However, AMIA is concerned about the proposal under the new access report requirement that, "…to the extent such disclosures are made through direct access to electronic designated record set information, such disclosures will be recorded and available to the individual in an access report under proposed 164.528(b)." Under this formulation, what the Department has given with one hand – an easing of the administrative burden on information-based research vis-a-vis the accounting of disclosures requirement – it has more than taken away with the other, by requiring inclusion in the access report of all uses and electronic disclosures of PHI for research, including uses pursuant to an authorization, uses approved by an IRB or Privacy Board, uses preparatory to research, and even uses in which the PHI utilized was restricted to a limited data set. As an association committed to responsible use of health data for research purposes, AMIA is astounded that by including research uses (and disclosures of electronic designated record set information) in the access report requirement, HHS has proposed not a reduction in the burden on research, but a significant increase – and we are hard-pressed to understand what the benefit of this requirement would be to an individual or to society.

  We are concerned that the NPRM could impede the ability to do research. It would be nearly impossible to track data that are exported for the purposes of research. Once the data are exported for analysis, there may not be any logging of who had access to those data. Similar exports are frequently necessary for conducting quality analyses as well.

  To track this type of access would almost be guaranteed to be a manual process. While researchers do file a request with an IRB in order to gain access to patient data, and the IRB records which individuals have access to the data, there is certainly no specific logging of access to the extracted data that would be readily accessible for reporting from an EMR.

- Will a shorter 30-day deadline, with a single 30-day extension, significantly benefit individuals, and will it place an unreasonable burden on CEs? How long have CEs needed to collect the information necessary for an accounting (including from BAs) and to generate an accounting of disclosures?

  The actual work involved is on the order of days, if the people involved are not doing anything else. In practice, requests can take weeks to fulfill. 30 days with a single 30-day extension would not seem to place unreasonable burden on CEs. The added value to individuals is unclear, but presumably depends on why they are requesting the information.

- HHS estimates the total cost for all providers nationwide to be approximately $20 million, which reflects an estimate that the average total cost for a CE to comply with the new rule will be $30. Are these reasonable figures? Why or why not?

  No. This figure does not consider the cost of re-configuring present systems, which will cost from hundreds of thousands to many millions for each hospital system, to say nothing of the costs to physician offices and other facilities.

  Further, to quote one of our members, "The idea of a $30 change in the notice of privacy practices (NPP) is absurd. Many organizations use a shared NPP across multiple institutions. Each change to the NPP involves over a year of committees and lawyers. It costs thousands, probably tens of thousands, of dollars. No organization of any size changes these without major legal advice. Even small groups will pay hundreds or thousands of dollars."

  To summarize, these calculations are not reasonable for a number of reasons: (1) should the number of requests for access lists be high, CEs could potentially foresee at least one staff member assigned to the job of generating the access lists, explaining the lists to patients, and responding to issues identified; (2) privacy and security programs are generally already short of staff and therefore adding these extra requirements will necessitate adding more staff at a cost greater than $30.00; (3) in the age of increased enforcement and the launch of the new Office for Civil Rights (OCR) audits, slim resources will already be diverted to addressing the OCR's efforts; and (4) efforts to modify systems and even the paper and electronic resources needed to respond to such requests will present further costs in addition to staffing needs.

Concluding Comments

Recognizing that the Department has the authority to make significant changes to the HIPAA rules, AMIA believes that the assumptions made by HHS in delineating a new right to an access report are fundamentally incorrect. Congress directed that individuals should have a right to be informed of disclosures of PHI made *outside the covered entity* for purposes of "treatment, payment or health care operations" and AMIA supports the idea that individuals should have an ability to understand the use of health information by covered entities or business associates beyond the CE to which the individual entrusted the PHI in ways that may impact their care or payment for their care or the general quality of care delivered. AMIA does not understand, and therefore does not support, the notion that individuals should be able to learn if specific persons have accessed their "electronic designated record set information" (which, practically speaking, will include all PHI) absent some reason to believe that such an access was impermissible or otherwise inappropriate. We further believe that the Department is off-base in asserting that generation of an access report will require minimal, if any, changes to existing information systems, and in asserting that the burden in aggregating data across multiple information systems into a single access report is reasonable.

Again, AMIA very much supports the reasonable modifications to the accounting of disclosures proposed in the NPRM. However, we believe that the proposed access report requirements would represent a fundamental and unnecessary change to a regulatory regimen that has been in place for nearly 10 years. Thus, AMIA suggests that HHS re-evaluate its proposal for a broad HIPAA access report [at §164.528(b)], and we encourage the Department to withdraw the access report provision of the proposed rule.

As a source of informed, unbiased opinions on policy issues relating to the national health information infrastructure, uses and protection of clinical and personal health information, and public health considerations, AMIA appreciates the opportunity to submit these comments. Again, we thank the Department for soliciting public input. Please feel free to contact me at any time for further discussion of the issues raised here.

Sincerely,

Edward H Shortliffe

Edward H. Shortliffe, MD, PhD
President and CEO, AMIA

AMIA is the professional home for biomedical and health informatics and is dedicated to the development and application of informatics in support of patient care, public health, teaching, research, administration, and related policy. AMIA seeks to enhance health and healthcare delivery through the transformative use of information and communications technology. AMIA's 4,000 members advance the use of health information and communications technology in clinical care and clinical research, personal health management, public and population health, and translational science with the ultimate objective of improving health. Our members work throughout the health system in various clinical care, research, academic, government, and commercial organizations.