ACP
American College of Physicians
INTERNAL MEDICINE | Doctors for Adults®

July 26, 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 College of Physicians (ACP), I am writing to share our views on the **HIPAA Privacy Rule Accounting of Disclosures Under the Health Information Technology for Economic and Clinical Health Act (HITECH) Notice of Proposed Rulemaking (NPRM).** ACP is the largest physician specialty society and second-largest physician membership organization in the United States. ACP represents 132,000 internal medicine physicians and medical student members. Internists specialize in primary and comprehensive care of adolescents and adults.

General comments:

ACP is pleased to note that this NPRM clarifies and simplifies the requirements related to Accounting of Disclosures. In general, it appears that OCR has wisely taken the approach of describing limits on the types of disclosures rather than listing exemptions to the requirements. Further, ACP agrees with the goals of providing patients with appropriate and timely answers to their questions regarding disclosures of their healthcare information. However, we believe that OCR has chosen a technology with which to achieve the appropriate goals that will be challenging to use for this purpose.

As we understand it, OCR proposes to re-purpose a technology, an access log, which was designed for use by technical experts to monitor system activity, and require it to serve the purpose of allowing individuals to understand how their records are being accessed and used. In the absence of data demonstrating that use of the technology for this purpose is both valid, affordable and practicable, additional study, development, and testing will be required before its use can be credibly required. We are unaware of any standards in general use that address the form, syntax, semantics, recording, management, or use of system access logs. Rather than proposing a requirement to use an untested technical approach,

we recommend that OCR instead propose that that this technology be extensively studied and standardized before requiring its use.

For access logs to be useful for patients and manageable for clinicians and practices, all required functions should be automated and generated directly from the certified EHR technology in use. OCR should specify the standards for the content and management of required logs. These specifications should be added to EHR certification criteria. Certified systems that include automated functions to generate reports in specified formats must be available in the market. Once all of this has been accomplished, the proposed approach can be studied. Certification criteria must completely specify the proposed requirements in this rule, and the criteria must be required for certification. No requirements should be imposed on providers until they have systems capable of capturing and reporting the information required.

As these proposed rules are onerous and apply only to providers using EHRs, this serves as a clear disincentive to those who have not yet committed to EHR implementation. The burden of complying with these rules in the absence of mature automated functions in EHR system is unreasonable and will lead rational decision makers to forgo EHR implementation until such capabilities exist.

We believe the proposed rules as written will have the unintended negative consequence of reducing the clinically appropriate and necessary sharing of PHI with adverse impact on patient care quality and safety. Providers will likely resort to printing and handing records to patients for them to deliver to other providers rather than having to explain cryptic listings of record accesses in a log file.

Finally, given all of the new burdens being placed on practices with EHR systems (Meaningful Use Stages 1, 2, and 3; 5010 and ICD-10; quality reporting required by CMS and other payers and oversight bodies; new reporting requirements from other public agencies; and others, including reporting to state and specialty boards) this proposed rule is ill-timed, placing an unacceptable additional burden that may well threaten the achievement of these other important goals.

Specific Comments:

In the table below, we have identified specific requests for comment in the left column and provided our specific comments in the right column.

IV. Description of Proposed Rule **A. Accounting of Disclosures of Protected Health Information – Section 164.528(a).** **1. Right to an Accounting of Disclosures**	**ACP Comments**
We request comment on our 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.	The meaning of "designated record set" is not clear. A more specific definition, including examples of included and excluded systems is required. This rule should only apply to those data that are actually stored in the EHR (as an example: the data from an external system that are not releasable via the EHR would not pertain – all the numerical, imaging and tracing data that may go into a final summary report but could not be released from the EHR directly – but only the final report and any data that are included as part of it (images, tracings, T-scores, etc.). If these

25 Massachusetts Avenue, NW, Suite 700, Washington, DC 20001-7401, 202-261-4500, 800-338-2746
190 North Independence Mall West, Philadelphia, PA 19106-1572, 215-351-2400, 800-523-1546, www.acponline.org

	background data are not part of the Legal Medical Record per se and cannot therefore be released from the EHR, they should be excluded.
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 of disclosures beyond three years**.	This needs to be consistent with the statute of limitations in each state, which generally starts at the point of discovery. But all other requests for information could be restricted to 3 years. 95+% of the accessing and reporting burden resides in having to do it at all, with the specific volume and specific duration coming into play mostly when it has to be retrieved, organized or presented manually. It quickly becomes an unmanageable burden if it has to be done manually, whereas it could be straight-forward and non-burdensome if it can be automated from the EHR and better yet, available in a patient portal where patients can review on demand rather than requesting a report from the entity. The next layer of burden would be the patient who then contacts the practice or hospital and wants an explanation for those who accessed the chart…a potentially huge burden. We have seen one estimate of >150 distinct individuals legitimately needed to access a patient's chart in one way or another for a single hospitalization.
We request comment on the burdens on covered entities and benefits to individuals associated with also receiving an **accounting of disclosures that includes information provided in accordance with the breach notification requirement.**	The burden to CEs will depend on how automated this process can be. Also, it seems that if one is required to report breaches through a different mechanism already, having to do so in here is redundant. If it involves no effort because it is automated, it may not be a significant burden, especially if it can be programmed to include evidence of the date, time, etc. of notification of the individual done by other means.
We also propose to continue to include in the accounting requirement disclosures for public health activities (except those involving reports of child abuse or neglect). . .	Should other abuse/neglect examples also be exempted? (elder, spouse)
We request comment on our proposal to **exclude these categories from the accounting of disclosures requirements,** including comment on the rationales expressed below, and will revisit these exclusions in drafting the final rule based on the public comment we receive.	It is not clear why any of these disclosures should be hidden from the patient. Some concern about proxy access, especially if proxy could be abusive, neglectful, or otherwise take advantage of the information to the detriment of the patient. It appears that that this change entitles these entities to gain information from the EMR without notification to the patient. If this is the intent, we

25 Massachusetts Avenue, NW, Suite 700, Washington, DC 20001-7401, 202-261-4500, 800-338-2746
190 North Independence Mall West, Philadelphia, PA 19106-1572, 215-351-2400, 800-523-1546, www.acponline.org

	would object. We are concerned with the implications of the "disclosures for research purposes. I Please provide a layman's interpretation of that proposed exemption on the conduct of medical records research and population-based studies that are typically deemed exempt in human subjects protection. This section is not written clearly enough for us to comment comprehensively.
We thus solicit public comment on the **value of the current accounting for research disclosures** to individuals who have used or might in the future request such an accounting, including comments on what may be the most important/useful elements of the current accounting to individuals. . . Further, we seek public comment on **alternative ways that we could provide the individual with information about the covered entity's research disclosures**, such as the IOM's recommendation for a list of all IRB/Privacy Board approved studies, or whether other types of documentation about the research could be provided to the individual in a manner that is potentially less burdensome on covered entities but still sufficiently valuable to individuals.	More specific proposals would be required for us to make informed comments. In general the precedent that most medical records research is not "human subjects research" has a long and strong history. That patients would have a *right* to know in every possible way their (typically deidentified) medical information is being used seems to invoke a view of rights that is a bit strong. It also could lead to unanticipated consequences related the completeness of population-based data sets. We would favor notification to the patient that their information has been obtained for research. However, if the patient has given broad permission to use their data without identifying information prior to delivery of the data to the researchers, this seems sufficient. On the one hand, it can be argued that if the risk is so low that an IRB has waived the requirement for individual authorization, then there is little chance of benefit and only burden to requiring accounting or reporting. On the other hand, if it is no more difficult to make this information available than not, the spirit of the rule is to let patients know when their information is disclosed for any purpose, and let them give feedback suggesting whether the IRB was correct or not in terms of its estimate of risk or impact to the patient. Again, our response would differ depending on the effort required for reporting.
We also propose to not include disclosures for **health oversight activities** under § 164.512(d).	Those patients who distrust government in general (and there are more than a few) will be most interested in which government agencies are seeing their PHI. Unless the transmitted information is de-identified by HIPAA criteria, such patients who care about disclosure reporting at all would want this kind of disclosure included. The argument that you can exclude "routine" disclosures is something

25 Massachusetts Avenue, NW, Suite 700, Washington, DC 20001-7401, 202-261-4500, 800-338-2746
190 North Independence Mall West, Philadelphia, PA 19106-1572, 215-351-2400, 800-523-1546, www.acponline.org

	we'd like to make for why we shouldn't have to disclose for "treatment, payment, and health care operations" as was the case in the paper world. If the government is a potential recipient of the same kinds of questions patients will ask providers about who Mary Smith is (the person who roomed the patient), and why she accessed the chart (to record vitals and a chief complaint), they will have a better sense of the impact on providers as end users and it will inform more realistic rules on what needs to be reported for the purposes of treatment, payment, and health care operations. Just because an EHR (may) make it easier to do so doesn't necessarily make it wise.
As indicated above, we believe that **disclosures for law enforcement purposes and judicial and administrative proceedings** directly implicate an individual's legal and/or personal interests and thus believe the individual should have a right to learn of such disclosures.	We make the same arguments as above…to the extent that individually identifiable health information (IIHI) is released, it is fair game as long as it can be reported automatically, and that patients and families of decedents will have more interest in this than the framers think. This applies equally to disclosures about decedents to coroners, medical examiners, and funeral directors.
2. Content of the Accounting	We agree with the proposed changes with the following caveats. We want to confirm that you are only referring here to disclosure (release) to an outside entity, NOT access to information by an internal member of the same organization using the same EHR – would be far too burdensome. As stated repeatedly in our comments, our support is dependent to the extent that systems are required to support these functions in a totally automated way.
3. Provision of Accounting	This is only reasonable if there is ***virtually no work required*** on the part of the entity with qualified EHR technology to respond to such requests. In fact, it should be achievable through a self-service component of a patient portal. The data should be no older than ***one month*** (<u>not</u> 30 days), and allowing for this self-service component on a portal would eliminate the work and the charge issue. The reasonable charge for having to do a manual accounting of disclosures could be really expensive for patients. In the absence of certified EHR with automatic report generation, the fair market costs could easily be $250 or more given the reporting burden of the proposed requirements How is a practice supposed to know and be able to account for disclosures by business associates

25 Massachusetts Avenue, NW, Suite 700, Washington, DC 20001-7401, 202-261-4500, 800-338-2746
190 North Independence Mall West, Philadelphia, PA 19106-1572, 215-351-2400, 800-523-1546, www.acponline.org

	unless this is referring to direct release from EHR to someone else by a BA? If released to a BA who then keeps it separate and releases it later, how would a practice be able to know and report it? Either we do not understand this provision, or it is completely unworkable. If a patient makes a second request thirteen months after the first request, we assume the practice would only have to report on any access since the last request rather than the prior three years. Is this correct?
B. Right to an Access Report – Section 164.528(b) **1. Right to an Access Report**	This scheme represents a massive new administrative burden that will extend far beyond just generating and sending a report. The number of unknowns in this proposal is large. What does it mean for a report to be "understandable to an individual"? The patients most likely to want to see a report are also most likely to require extensive explanations and follow-up on the entries. Extracting subsets of data from access logs and merging extracts from different access logs will be significantly more time-consuming and expensive than the Department assumes. For small practices without on-site IT expertise, such expertise will have to be hired to fulfill each request. Access logs are not like databases where a "point-and-click" interface can be used to construct a report. Recent research (cite JAMIA) found that extracting accurate data from access logs is problematic. Interpretation of the raw data may be required. The Access Report requirement should not be implemented until there is wide industry experience with their use. Has there been any research or testing of this in the real world with real names, to see how many a person could identify, even though in an analysis all would have accessed the record appropriately? Despite this, viewing such a list for some patients will raise concerns, confusion and worry, (in the vast majority of cases, needlessly) because they will see names and roles they do not know, leading to requests for burdensome explanations of: 1. Who I am 2. What my role is 3. Why I accessed your chart at that particular point in time (assuming I can remember…)

25 Massachusetts Avenue, NW, Suite 700, Washington, DC 20001-7401, 202-261-4500, 800-338-2746
190 North Independence Mall West, Philadelphia, PA 19106-1572, 215-351-2400, 800-523-1546, www.acponline.org

	4. Why I needed to send this information to A, that information to B, etc. We see this as a potential iceberg that many folks will crash into – leading to big increases in valueless-added work in the name of security and privacy.
2. Content of the Access Report	While due regard is being paid to the privacy needs of patients, it is important for the safety and well-being of care providers and their families to be considered as well. The access log must not be allowed to become an aid to stalkers or worse. Only the minimal information needed to correctly identify the individual responsible for an access should be included. On the other hand, it may be quite useful to identify the general role of the individual accessing a record, and this is likely to reduce dramatically the concerns of patients and the burden they place on provides with follow-up questions regarding particular accesses. Again, the key to decisions regarding inclusion of data elements should be driven at least in part by the amount of effort required to collect it or to answer questions about it. If a data element is not already routinely collected in the course of normal operations, we can expect that significant cost and time will be expended by practice staff, system vendors and IT consultants to make the collection and reporting happen properly. These costs have not been captured adequately in the calculations. Keep in mind that all of the activities discussed in this section of the proposed rule represent new un-reimbursable costs to practices not matter how much the activities can be automated. The costs of all programming effort by vendors and consultants, along with an element of profit, will be passed along directly to practices.
We request 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. We additionally request comment on ways in which such accesses, if excepted from the access report, could be identified and excluded in an automated way.	We agree with the proposal not to require description of purpose of access. A suggestion for the future would be to explore the feasibility, benefits, risks and burdens of systems being able to automate capturing the "context" in which the access was made. More likely legitimate access would include in the context of an office visit, telephone encounter, prescription renewal, referral, etc., while a higher risk context would be simple opening and reviewing a chart without

25 Massachusetts Avenue, NW, Suite 700, Washington, DC 20001-7401, 202-261-4500, 800-338-2746
190 North Independence Mall West, Philadelphia, PA 19106-1572, 215-351-2400, 800-523-1546, www.acponline.org

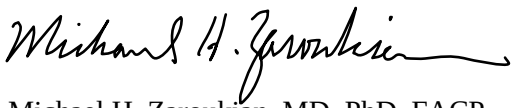
	taking any other action (higher risk that someone was "snooping around")
However, we believe that this administrative burden is reasonable in light of the interests of individuals in learning who has accessed their protected health information. Additionally, the burden of generating access reports will 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.	We disagree. The burden is far too high. Furthermore, we believe it is not necessary to provide an aggregated report for patients to have information they can understand and use. The requirement should be to make each report understandable to the patient (with a clear definition of what "understandable" means), not to aggregate them all. For example, individual lab test result reports may be provided to patients now, but aggregating individual reports from different labs and different times into a common format is not necessary or sufficient to ensure that the report is understandable. You have not provided evidence that understandable but separate reports are too confusing or burdensome to patients or that an aggregated report will be that much more useful/helpful to the patient. Given the burden, we would like to see evidence that not aggregating the reports is already a problem for patients and that this solves a problem that needs to be solved.
We are also proposing, in paragraph (b)(2)(iii), that the covered entity provide the access report in a **format that is understandable to the individual**.	This is simultaneously too vague, in the eye of the beholder, and potentially unachievable for a given patient. The format requirements need to me made clear, preferably with examples. Please do not require multiple formats of reports or require the capability to extract subsets of accesses from the logs. At least as an initial test, allow a single format and complete data for a given time frame to be the only reporting specifications. Small practices do not have the IT capabilities to perform any data manipulation not completely automated by their EHR system.
3. Provision of the Access Report	Once automated, we could imagine an entity generating a monthly report, which technically could violate a 30 day requirement. We suggest rewording to "such reports must be made available to patients on at least a monthly basis". Small practices are likely to require 60 days for initial reporting, especially if this is the first time an office has been asked to generate the report for a particular patient.
We are proposing at paragraph (b)(3)(ii) that the covered entity must provide the access report in the **machine readable or other electronic form and**	We have no concerns about providing an access report in one of these formats per se. However, we have some concern that the report could be altered

25 Massachusetts Avenue, NW, Suite 700, Washington, DC 20001-7401, 202-261-4500, 800-338-2746
190 North Independence Mall West, Philadelphia, PA 19106-1572, 215-351-2400, 800-523-1546, www.acponline.org

format	by patients leading to problems. We would prefer to see a document format that could not be altered by a patient without any evidence of the alteration.
As with the accounting of disclosures, we are proposing that the covered entity may **not charge** for providing the first access report to an individual in any 12-month period, but may charge a reasonable, cost-based amount for each additional access report that is requested within the 12-month period (which may include the reasonable costs of including access report information of business associates). We are also proposing, in paragraph (b)(3)(iv), that the covered entity may require individuals to make requests for an access report **in writing** provided that it informs the individual of such a requirement.	This naturally depends on the cost of providing the report. When automatically generated from EHR and minimal cost to covered entity, this could be fine. If it has to be manually collected, merged, formatted, inspected for accuracy and burned to disc and/or printed at a total cost of hundreds of dollars, it would be a significant and unacceptable cost burden even to provide the first report. We support allowing the covered entity to require written request.
V. Effective and Compliance Dates	All compliance dates should be extended as long as possible. Many providers and covered entities are drowning in the demands of getting all of the other requirements met. This one will be a beast if it is not automatically achievable from the EHR directly. Most practices are unaware that this new set of unfunded burdens is even under consideration.

ACP strongly supports patients' rights to understand by whom and how their healthcare information is used. We urge that all requirements to collect, gather, and report accesses and disclosures to patients recognize the capabilities and limitations of the health information technologies available to practices – large and small. We further recommend that only those audit and disclosure technologies proven to be accurate and reliable that are part of a certified EHR and from which reports of disclosures and releases can be automatically generated should be required. Anything else creates an unacceptable reporting burden and will discourage practices to adopt EHR system. In addition, not enough is known about the actual costs and effort that will be required of practices to meet what is generally acknowledged to be a relatively rare request.

Sincerely,



Michael H. Zaroukian, MD, PhD, FACP
Chair, Medical Informatics Committee
American College of Physicians

25 Massachusetts Avenue, NW, Suite 700, Washington, DC 20001-7401, 202-261-4500, 800-338-2746
190 North Independence Mall West, Philadelphia, PA 19106-1572, 215-351-2400, 800-523-1546, www.acponline.org