



233 N. Michigan Ave., 21st Fl.
Chicago, IL 60601-5800

phone » (312) 233-1100
fax » (312) 233-1090
web » www.ahima.org

March 12, 2010

David Blumenthal, MD
Office of the National Coordinator for HIT
Attention: HITECH Initial Set Interim Final Rule
Hubert H. Humphrey Building, Suite 729D
200 Independence Avenue, SW
Washington DC 20201

RE: RIN 0991 –AB58
Standard on Accounting of Disclosures

Dear Dr. Blumenthal:

The American Health Information Management Association (AHIMA) would like to comment specifically on the standard for the “accounting of disclosures” as included in the January 13, 2010, *Federal Register* Interim Final Rule (IFR) on HIT: Initial Set of Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology.

The issue of accounting of disclosures is very important to our profession, and members have asked that we address it separately. AHIMA will be sending an additional letter commenting on the over-all IFR. AHIMA is a not-for-profit professional association representing more than 56,000 health information management (HIM) professionals who work throughout the healthcare industry and across all sectors of healthcare providers. HIM professionals are educated, trained, and certified to serve the healthcare industry and the public by managing, analyzing, reporting utilizing and protecting data vital for patient care, while making it accessible to healthcare providers and appropriate researchers where it is needed most. The confidentiality and security of health information has been a cornerstone of the profession’s concerns with the use and disclosure of healthcare data and information. Likewise, over the last two decades AHIMA has collaborated with all the applicable agencies, offices, and committees of the Department of Health and Human Services that have been addressing privacy issues.

As the Office of the National Coordinator for HIT (ONC) noted in the January 13, 2010, IFR the individual request for an accounting of disclosures, under the HIPAA requirements since 2003, has been minimal. While AHIMA has not conducted a formal survey in recent years; when such surveys were done the requests for such an accounting rendered a response of 1 or 2 inquiries per provider at most in a year. Most organizations reported zero.

The results of the surveys conducted demonstrated there was a lack of demand for the accounting of disclosures and therefore many providers kept this information manually.

It was due to this lack of demand and limited use of electronic records, as well as the narrow number of categories that required an accounting under HIPAA that caused most provider organizations to keep an accounting manually; usually in the HIM department in hospitals or directly in the paper record in many physician practices and other small provider sites. Today, most provider organizations do not use the EHR/EMR to track disclosures and much of the accounting remains manual. This lack of demand means that few vendors have been asked for such a modification to existing EHR systems or inclusion in new systems.

Specific comments on the IFR standard:

III. B. 8. Definition of Disclosure (75FR2023)

We understand the definition remains within the HIPAA rule; however, when applied to treatment, payment, or operations, it raises a number of questions and concerns:

- What is the definition of an entity? Is it a specific provider or would it cover the enterprise? Will it include transfer of protected health information (PHI) to Business Associates (BAs) and potentially to BAs of BAs?
- Will it include the typical transfer of PHI to ancillary services outside of the entity such as laboratories? Will these referral labs, likewise, have to keep such information?
- If a hospital has established an EHR network with physicians not considered employees or resident medical staff of the hospital, would physicians in this network be considered part of the entity, raising the potential that even transfers within an EHR enterprise network or HIE network will need to be tracked for an accounting?
- While the certification standards apply to the EHR, many of the disclosures possible under our interpretation come from systems outside of the EHR (i.e. registration, admissions, patient accounting, physician accounting). Some disclosures, being verbal, must be accounted for in a separate system. Is it ONC's intention to see all of this data being transferred or resident in the EHR? This question also raises the issue as to other requirements under the IFR and the potential requirements under Meaningful Use that appear to address other administrative functions outside of the EHR such as eligibility and claims. Is it ONC's intention to suggest that an EHR is all of the records within the medical enterprise or at a minimum any system that contains PHI?
- There is considerable concern by our members that the accounting called for in this proposal will eventually turn into a request for identification of all users of the data, not just those who fit under the definition as stated. This may be another very expensive workflow process change and if this is under consideration we would like to raise the issue now.

III. C. 2. c. Privacy and Security Standards (75FR2034)

The adopted standard for Record Treatment, Payment, and Health Care Operations Disclosure is straight forward. However, there are a number of questions and concerns that this standard raises.

- Date and time are simple standards – how will they be represented?

- Patient identification (name or number) – how will name be represented and what number will be needed by an entity versus, perhaps a Health Information Exchange Organization (HIEO) or a BA? How far can a request for an accounting go to the various entities in one of these paths where we need to be concerned about using the same identifying number?
- User identification (name or number) – will each organization be expected to maintain its own system of numbering these users or will we have to use Medicare numbers for professionals, IRS numbers, etc?
- Description of the disclosure. Of necessity this needs to be a coded process. Will the ONC or some other body adopt a code set for use under description to have some sense of where data is being disclosed across the industry? When an organization, even a small practice begins to account for almost all outside disclosure this will amount to hundreds to thousands per day. Even coded data will take up considerable space. If a code set is developed how detailed might it be? For example, under a payment reason code would “claim” suffice, or would it have to be detailed as to primary claim, secondary claim, resent claim, etc? Simplicity and uniformity need to occur or the administrative costs associated with this accounting will quickly increase and add burden to the cost of health care considerably.
- Since this data might not be collected in the EHR system we request clarity on whether this means non-EHR systems will need to be certified?

III. C. 4. c. Certification Criterion and Standard Regarding Accounting of Disclosures (75FR2036-37)

In describing the HITECH requirements for the Secretary to propose modifications to HIPAA within 6 months, you note that this is to “require HIPAA covered entities account for disclosures related to treatment, payment, and health care operation made through an electronic health record and to identify in the regulations the information that shall be collected about each of the disclosures” (underline added).

This again raises several questions and concerns:

- Can we presume that de-identified PHI need not be included in any accounting and if so could reporting to registries or researchers, using a sender number to represent the patient (with no key to the registry) be sufficient so that transaction would not have to be considered a disclosure?
- If a disclosure is made along with data taken from the EHR but originates from another non-EHR system, does this count as one of the newly covered disclosures? We think there is an obvious answer, however it points to the definition of what is and what is not in the EHR system, and what systems will have to be monitored and organized to provide an accounting.
- The trigger on compliance rests with the purchase of an EHR, but as we are pointing out through our questions there are many systems that are involved in the disclosure of PHI in a healthcare provider or health plan setting, and many of these are legacy systems which will have to be retrofitted to begin the process of accumulating this data. In tertiary care facilities and university hospital systems this collection of systems will have to be networked across a variety of different systems such as billing, practice plans, admissions and registration to name a few. While much of the release of information that had to be tracked under the original HIPAA requirement came through the HIM department, treatment information flows from a variety of medical staff interacting with referral physicians, consulting physicians and

others, outside of the record process. Claims and claims follow-up can be distributed as are operations activities and reporting. So the question becomes one of defining entity and how much the healthcare system is willing to pay for this accounting? While the data to be collected is as you say “basic,” the means to collect such data across systems is not.

- We share and appreciate ONC’s concerns that “several significant technical challenges will need to be addressed” and AHIMA also shares the concern for the amount of electronic storage that will be necessary to record three years worth of information and the impact this collection process and function will have on the performance of the various systems that must be linked. We know there are audit functions in existence in many systems, but these systems have not been designed to define disclosure under the definition currently in existence or the revised one as defined in the IFR.

AHIMA suggests that it would be helpful to the healthcare industry and consumer to understand the issues and costs that are associated with the accounting of disclosure requirement, both to retrofit a system into existing EHR systems as well as systems coming into adoption. In both cases this would have to include all of the systems in an entity that must be used to track disclosure from the entity, not just the EHR system.

We recommend that the HIT standards committee examine this issue promptly, and with the HIT Policy Committee and your office, make recommendations as requested by Congress under HITECH to make modifications that will allow for the intent of this accounting to come to realization, but in a timetable that recognizes the technology limitations and the costs associated with implementing this data collection system. While certainly there are systems out there with the capability to do this function, they are not necessarily residing in the healthcare industry and not designed to accomplish the task described above.

AHIMA agrees that consumers have a right to know to whom their record may have been disclosed. However, as discussed above this accounting in today’s healthcare system does not occur easily, without significant costs or major delays in the transfer of this information through a centralized process. Over a period of time the healthcare system will change its systems and as these systems change, technology to make such an accounting can be implemented; however in the current time table with the number of legacy systems and costs of adopting new systems, we do not believe this is a task that can be completed in the time required by Congress and not without significant cost to the healthcare industry.

Subpart B – Standards and Implementation Specifications for Health Information Technology (75FR2045-2047)

§ 170.200—170.210

The proposed standards for EHR certification do not address standards for basic EHR functionality, but are targeted to specific functionality in certain areas such as content exchange, vocabulary, and transport for HIE. Although new standards are identified for privacy and security, they are focused on user identity and transmission security in the context of health information exchange activities, and not the integrity of the source system.

There was an EHR certification body (CCHIT) promulgating standards prior to the HITECH Act. Detailed certification criteria were developed for both inpatient and ambulatory EHRs. HHS made a conscious determination to not adopt previously recognized certification criteria developed in 2006 in their interim final rule. We believe that the new HHS standards leave a large gap between the previous standards, and the limited areas where standards are now proposed.

Two of the stated goals of EHR adoption include:

- “Improving quality, safety, efficiency, and reducing health disparities”, and
- “Ensure adequate privacy and security protections for personal health information”

The proposed regulations define standards for data integrity for data exchange activities, but not for the underlying source system which produces the data that will be exchanged.

We are concerned that the proposed standards will not adequately support the stated goals of health care improvement and adequate privacy and security because of missing foundational requirements for EHR systems and modules. Meaningful use will not be effectively achieved if the underlying data is not accurate, complete, and of unassailable integrity. The government has not identified any standards for underlying EHR systems or modules that support system and data integrity, authentication standards, and non-repudiation.

AHIMA recommends that ONC identify standards for underlying EHR functionality, such as those previously defined by CCHIT or those found in the HL7 EHR System Functional Model (EHR-S FM). The standards should be detailed enough to support the goals of the Federal government in the areas of user identification, access and validation, validity of data and data support structures, and be supportive of fraud detection through a foundation that allows for validation and authentication of all system activities.

§ 170.210(b) Record Actions Related to Electronic Health Information

To ensure appropriate application of the record action (and related audit log), clarification is needed on the definition of “user identification.” If user ID is meant to reference the “author(s)” or “contributor(s)”, we recommend that terms be aligned with existing standards, such as those used in the HL7 CDA, for consistency.

The IRF should reflect the need to collect record actions when health information is “viewed” as required by the HL7 EHR-S FM standard. An alternative to the term “view” is the term “read.” The HL7 EHR-S FM defines this term and includes the following record actions: view, report, display or access.

The reference to printing leaves it unclear as to the intention of the rule. Printing is only one type of output/disclosure format used by EHR systems. If the intent is to track disclosures through the audit log then the rule is leaving out many other disclosure types and will not result in comprehensive logging of these record actions. Other disclosure types include report generation, extraction, and exchange. Disclosure may also be in the form of copying a report to a CD or an e-mail. It can also be in the form of allowing access to a report through a patient portal.

The record action “viewing” is an important action in support of privacy and security priorities in the IFR and NPRM for meaningful use.

Record actions for output of electronic health information should not be limited to printing. The rule needs to use a more inclusive term to include extraction, exchange, report/.pdf, as well as printing.

The lack of record action data on viewing and printing will result in a significant gap or loophole for individuals who wish to inappropriately access protected health information. Record action data provides critical information in support of the confidentiality, privacy and security program for a health care provider.

As a result, AHIMA recommends the following:

- 1) Define the term *user identification* and consider modifying the term to *author(s)*.
 - Utilize existing definitions contained in standards such as HL7’s definition of author which includes a person, organization or device.
 - Regardless of the term used, it should be plural to recognize that records can have more than one user ID (author or contributor) assigned to it. If the term *user identification* continues to be used, a definition is required. If it is synonymous with *author*, then the need to capture more than one *user identification* component must be recognized.
- 2) Add a new record action for *reading* or *viewing*.
- 3) Clarify the intent of capturing the record action *printing*. Consider expanding the record action to include the other types of output methods rather than the limited and narrow method of printing.

§ 170.210(e) Record Treatment, Payment, and Healthcare Operations Disclosures

In reviewing the required elements for an accounting, it was noted that the rule missed requiring an important piece of information for an accounting of disclosures – **who** the PHI was disclosed to. AHIMA strongly recommends adding this component to the accounting of disclosures requirements.

In addition, the definition of a disclosure for treatment, payment, or healthcare operations includes providing access to information. The record action data does not require collecting “read/view/access” which would be necessary in supporting accounting of disclosure functionality in an EHR module/system. Furthermore, the difference between a use and disclosure is not adequately defined by the rule to determine when an accounting is triggered.

As a result, AHIMA recommends adding “Read/View” as a record action in 170.210(b) to support the accounting of disclosure requirement.

Subpart C – Certification Criteria for Health Information Technology
§ 170.302(r) Audit Log

Systems have the capability and system administrators routinely “turn off” audit logging processes to increase system performance and address storage capacity issues. As audit data are used to support record integrity, compliance activities related to breaches, and inappropriate access, it is critical that audit logs be required during routine operations of the system, data be maintained in a secure manner, and data be accessible in a human readable format. Many systems have logs but are often difficult to access (or can only be accessed by the vendor through special processes and with expense). Not addressing accessibility and security as part of the requirement will result in a mandate that is critical but may not be fully realized by the healthcare provider depending on the vendor that they select.

Additional requirements are needed to support the intent and purpose of the audit log for record integrity purposes and ensure that a minimum set of audit logging procedures are completed.

AHIMA recommends the following requirements be added:

- Always be on during normal production for the minimum elements specified in 170.210(b)
- Maintained in a secure manner and alterations to the log tracked.
- Produced in a human readable format.
- Retained in conjunction with the retention period of the record.

Conclusion

As many in the healthcare and information industries know, adopting and implementing an effective but conservative accounting system for disclosures will be a significant challenge for system users and vendors alike, especially given the number of transactions that occur on a daily basis. Health information flows in many different media as needed to provide diagnosis of and clinical care to patients. Such information and data not only provide the information used to run our health systems – to improve patient safety, supply knowledge for medical decisions and improve quality and efficiency, but also for uses external to the organization for public health, health reporting, research, and reimbursement. The number and types of transactions vary immensely as do the size of the organizations and with whom they interact.

We urge the ONC as well as the Office of Civil Rights and the Secretary to also consider our comments and questions (above) and balance the necessity to achieve confidence and trust in our healthcare information confidentiality and security efforts while not imposing a system of accounting requirements that could negatively affect the goal and objective for electronic health information.

AHIMA appreciates the opportunity to comment on these Accounting of Disclosures standards and the issues raised by ONC. If AHIMA can provide any further information, or if there are any questions or concerns with regard to this letter and its comments, please contact me at (202)659-9440 or dan.rode@ahima.org, or in my absence please contact either Allison Viola, MBA, AHIMA, AHIMA’s director of federal relations, at the same number or allison.viola@ahima.org, or contact Donald Mon, PhD., AHIMA’s vice president for practice leadership at (312)233-1135 or don.mon@ahima.org.

Our thanks for all of your efforts and for your time and consideration of these comments.

Sincerely,

A handwritten signature in blue ink that reads "Dan Rode". The signature is fluid and cursive, with the first name "Dan" and last name "Rode" clearly legible.

Dan Rode, MBA, CHPS, FHFMA
Vice President, Policy and Government Relations

CC Donald Mon, PhD
Allison Viola, MBA, RHIA