Title: 2014 Edition EHR Accounting of Disclosures (AOD) Certification Criterion

Brief definition of requirement:

MU Stage 2 proposed language proposes to adopt AOD reporting criteria for the reporting as was articulated in Stage 1 Certification: As an **optional** certification criterion. However, MU requests public comment on three key items:

I. Should criteria be revised to be a mandatory certification criterion?

II. Can 2014 Edition EHR certification criterion be revised to include capabilities that would comply with the current HIPAA Privacy Rule accounting for disclosure requirements at 45 CFR 164.528?

III. What additional, changes to the certification criterion would be needed to support compliance with the proposed HIPAA Privacy Rule accounting for disclosure provisions as they were proposed?

Benefits of requirement:

- Requirement is simply to "Record disclosures made for treatment, payment, and health care operations in accordance with the standard specified in §170.210(d)." The standard only references the need to collect the date, time, patient identification, user identification, and a description of the disclosure for disclosures for treatment, payment, and health care operations.

- There are many benefits to the audit logging requirements described; these are mainly information security related and are only loosely associated with the AOD reporting requirement.

- There is benefit in keeping the "optional" certification criterion language so long as HHS and OCR have not identified a long-term plan for addressing what the AOD report should entail.

- It would not be a burden for the criterion to become mandatory so long as language was added that refers to the "current" accounting requirements as stated within the HIPAA Privacy and Security rules; however, MU should not interpret what is "currently" required as an Accounting of Disclosures since this is a moving target.

Issues associated with requirement:

- The MU AOD requirements appear to be combining two very different concepts in its requirement. The HIPAA Privacy rule surrounding the Accounting of Disclosures Report is not a technical requirement and in operations, is a manually prepared document that describes research projects, court documents that require delivery of medical records and descriptions of incidents involving other inappropriate disclosures of patient information.

- The MU appears to contemplate that the audit language from the HIPAA Security Rule should be used to help prepare those sections of the AOD report that involve disclosures made for the purposes of treatment, payment or healthcare operations. It is erroneous to believe that audit data can be used to meet this requirement.

- Audit data does not provide enough information to provide a "description of the disclosure" beyond whether information was read, written, printed, or deleted. It cannot explain the purpose of an access event nor can it collect information needed to decide – in an automated way – if an access event was a "use" or a "disclosure."

- Unless each access required a human input that asked users to identify a purpose and if the user was an employee or an affiliate at the time of an access event (some of our staff are both and their role would

change frequently when accessing data), a system log would not be able to be used for the purpose of AOD reporting.

- These arguments have been made to OCR and much debate remains about the possibility of extending AOD reporting to TPO. Until HHS and OCR can clarify these and other AOD related issues, it is not recommended that technical standards be enforced in MU.

Requested Comments:

Can 2014 Edition EHR certification criterion be revised to include capabilities that would comply with the current HIPAA Privacy Rule accounting for disclosure requirements at 45 CFR 164.528?

This would be fine; so long a certification did not give specific technical implementation criterion since the HIPAA Privacy Rule requirements are still undergoing revision.

Omnibus revisions to the HIPAA administrative simplification are pending release which may shed some light on how proposed language was or was not adopted. HIPAA may only be revised once a year, therefore, if AOD requirements are not clarified in this revision, it will not likely be better understood before 2013 at the earliest.

What additional, changes to the certification criterion would be needed to support compliance with the proposed HIPAA Privacy Rule accounting for disclosure provisions as they were proposed?

No. The rule, as proposed included new rights and requirements that were widely criticized by the healthcare and patient advocacy community. The proposed language is not likely to be adopted as drafted.

Recommendations re: requirement:

Attached is Intermountain's response to the AOD RFI from 2009. In it, we make a number of recommendations – highlighted are some of the most useful sections.

Office for Civil Rights
Attn: HITECH Accounting of Disclosures
Hubert H. Humphrey Building Room 509F
200 Independence Avenue, SW.
Washington, DC 20201

[Submitted electronically to regulations.gov]

Re: Accounting of Disclosures RFI - 45 CFR Parts 160 and 164, RIN 0991–AB62

To whom it may concern:

On behalf of Intermountain Healthcare, thank you for the opportunity to provide additional information related to accounting for disclosures (AOD) of protected health information (PHI).

Intermountain healthcare is a not-for-profit, community-based integrated healthcare delivery system headquartered in Salt Lake City, Utah that operates 23 hospitals, more than 140 clinics, and other healthcare services. Intermountain has approximately 31,000 employees and has about six million patients in our longitudinal EHR. SelectHealth, Intermountain's health insurance company, covers more than 500,000 individuals. Intermountain employs approximately 800 physicians and has another 2,500 affiliated physicians who practice at our facilities. Intermountain is recognized for its success in the provision of high quality, efficient clinical care.[1] We are also recognized for our pioneering work in the development and use of clinical information systems which are critical in enabling the provision of this efficient, high quality care.

Intermountain supports the intent of the Health Information Technology for Economic and Clinical Health (HITECH) Act and the goal of providing useful information to patients who wish to better understand how their PHI may have been disclosed and appreciate the opportunity to provide the following information in response to the questions posed in the RFI.

RFI Question Responses:

1) *What are the benefits to the individual of an accounting of disclosures, particularly of disclosures made for treatment, payment, and health care operations purposes?*

Answer: In our experience, a preponderance of AOD requests relate to a specific privacy concern and that patients requesting an AOD report are not particularly interested in obtaining an accounting of all disclosures of their PHI, but rather are interested in understanding if a specific disclosure occurred. From a Treatment, Payment, and Healthcare Operations (TPO) perspective, these requests are generally related to a suspected inappropriate access request. In some case, an AOD was requested when a patient is concerned about a privacy breach but either does not wish to get an employee in trouble or if a patient is unaware that they can lodge a privacy concern with our office of Business Ethics and Complaince. We have found that nearly all patients who with these types of concerns were satisfied with our privacy investigation process and that current AOD reporting, would not provide the information they are truly interested in obtaining.

---

[1] *An Agenda For Change: A Dartmouth Atlas White Paper*, John Wennberg, MD, Elliott Fisher, MD, et al., (The Dartmouth Institute for Health Policy and Clinical practice, Dec 2009): 5.

2) *Are individuals aware of their current right to receive an accounting of disclosures? On what do you base this assessment?*

Answer: Yes, patients are informed of both their rights to request an AOD and the limitations of what an AOD will provide them in our notice of privacy practices tri-fold (available at admission) as well as in our extended notice of privacy practices available by request or online.

3) *If you are a covered entity, how do you make clear to individuals their right to receive an accounting of disclosures? How many requests for an accounting have you received from individuals?*

Answer: We publish our notice of privacy practices on our public-facing website as well as have copies of our notice of privacy practices tri-fold available at each hospital and clinic admission desk. AOD is discussed in each of these publications and a toll-free number is supplied for patients to use to request an accounting of disclosure. We have had less than a dozen AOD requests in the last 7 years.

4) *For individuals that have received an accounting of disclosures, did the accounting provide the individual with the information he or she was seeking? Are you aware of how individuals use this information once obtained?*

Answer: No. We have received complaints that employee activities – particularly TPO activities – are not part of the AOD. Under the expanded AOD requirements, these "uses" would still not be part of the AOD. For the most part, AOD reporting includes disclosures made to state agencies, research purposes and law enforcement (subpoena requests). Many of our AOD requestors are often seeking information related to an employee or clinician of Intermountain as part of a domestic or civil dispute.

With respect to treatment, payment, and health care operations disclosures, 45 CFR § 170.210(e) currently provides the standard that an electronic health record system record the date, time, patient identification, user identification, and a description of the disclosure. In response to its interim final rule, the Office of the National Coordinator for Health Information Technology received comments on this standard and the corresponding certification criterion suggesting that the standard also include to whom a disclosure was made (i.e., recipient) and the reason or purpose for the disclosure.

5) *Should an accounting for treatment, payment, and health care operations disclosures include these or other elements and, if so, why? How important is it to individuals to know the specific purpose of a disclosure – i.e., would it be sufficient to describe the purpose generally (e.g., for "for treatment," "for payment," or "for health care operations purposes"), or is more detail necessary for the accounting to be of value? To what extent are individuals familiar with the different activities that may constitute "health care operations?" On what do you base this assessment?*

Answer: No to the question of to whom a disclosure was made. We feel that to include the name of TPO discloses in an AOD could pose a significant risk to the named health workers, particularly in rural areas where the ability to find and contact specific employees is enhanced.

An increased number of our AOD requests related to domestic or civil disputes. On many occasions, our privacy compliance investigators become de-facto enlistees in supplying evidence in legal cases. One of the reasons we do not name employees involved in breach notification cases is to limit to what degree our privacy notifications can be used as evidence in such legal actions.

We feel that a court order should be required to supply recipient names therefore should not be included in a patient- requested AOD. Further, we feel we have an obligation to protect our employees from harassment. Due to the lack of contextual information available related to why a TPO health worker may have accessed a record, a patient may feel justified in contacting health workers directly to determine the "reason or purpose" for a disclosure. We feel that if a privacy concern is raised based on AOD reporting, that the covered entity should be responsible for investigating such a concern on behalf of the patient.

Yes to reason or purpose for disclosure. However, it is currently infeasible to determine purpose and appropriateness of disclosures using automated means. In order to electronically capture a reason or purpose for the disclosure, a self-declared attestation for "reason or purpose" would be required at the time of each access event. Clinical care workers would need to navigate this attestation screen for every access event in order for this information to be captured in the audit logs and, therefore, be reportable in an automated way. This creates unacceptable hurdles and delays, resulting in diminished patient care.

We have experience implementing and supporting such a "use / disclosure need" attestation – we call this a "break the glass" activity. A "break the glass" attestation is presented to users and requires them to declare a purpose for access to a specific record. It is required when users attempt to access a record for a patient with whom an obvious clinical relationship is not evident (e.g., the patient has not presented at the facility where the employee works).

We feel that an attestation cannot be relied upon to definitively report on a "reason or purpose for the disclosure". An attestation is a self-supplied testimony that the clinician or health care operations support employee feels that he or she has a legitimate reason to access a record. There is no means to verify that the access is appropriate other than the clinician's attestation.

For those users for whom we do not require a "break the glass" attestation (e.g., work in a facility where the patient has a current treatment relationship), the relationship alone is not enough to determine if the employee has a "reason or purpose" for accessing the patient record or if the access were appropriate.

a) *How important is it to individuals to know the specific purpose of a disclosure – i.e., would it be sufficient to describe the purpose generally (e.g., for "for treatment," "for payment," or "for health care operations purposes"), or is more detail necessary for the accounting to be of value?*

Answer: In our experience, this would be sufficient. Most AOD requests (which almost invariably turn into a specific privacy complaint/concern) want to understand why a specific disclosure was made to a specific EHR user. In fact, most often, patients do not really want to know for what purpose a disclosure was made, but, rather, want to know at a higher level that disclosures were deemed appropriate or not.

b) *To what extent are individuals familiar with the different activities that may constitute "health care operations?" On what do you base this assessment?*

Answer: Based on the number of complaints related to "privacy violations" that are, in fact, part of health care operations, it appears that patients do not necessarily know what constitutes PTO. For example, we regularly receive complaints that sending account information to a credit agency or collection agency is a HIPAA violation.

6) *For existing electronic health record systems:*

a) *Is the system able to distinguish between "uses" and "disclosures" as those terms are defined under the HIPAA Privacy Rule? Note that the term "disclosure" includes the sharing of information between a hospital and physicians who are on the hospital's medical staff but who are not members of its workforce.*

Answer: There are system limitations, but a primary reason we cannot determine "use" from "disclosure" is organizational, rather than technical. For non clinicians, it is not difficult to determine if a user is an employee or an affiliated staff member. However, for physicians many times this is a blurred line and it is not always simple to evaluate whether, at the time of access, a clinician is working as a part time employee or an affiliate with hospital privileges. We have many "dual-hatted" physicians. We also have many physicians who have purchased/licensed use of our EHR, therefore would fall under the "use" category even though they are not workforce members. This variable information is not readily available, nor could be definitively reported in an automated way.

b) *If the system is limited to only recording access to information without regard to whether it is a use or disclosure, such as certain audit logs, what information is recorded? How long is such information retained? What would be the burden to retain the information for three years?*

Answer: in accordance with 45 CFR § 170.210(e) the EHR system records the date, time, patient identification, user identification, and a description of the disclosure. The description is limited to what screens within the EHR were accessed, written to, or printed. Log data is retained for approximately 1 year. The burden for retaining data for the 3 years suggested is significant considering we log approximately 15-23 Million security (access) events a day. The issue with retaining more data is not just a factor of storage costs, but is also a factor of processing and parsing speed. More data means that our reporting takes considerably longer to comb through the audit logs to find the data for which we are reporting. Some investigation reports already run at well into the hours – querying larger repositories will make queries impossible to support using current technologies.

c) *If the system is able to distinguish between uses and disclosures of information, what data elements are automatically collected by the system for disclosures (i.e., collected without requiring any additional manual input by the person making the disclosure)? What information, if any, is manually entered by the person making the disclosure?*

Answer: The EHR is not able to distinguish between use and disclosures (as described above). All non TPO disclosures are currently manually entered into an independent AOD reporting database.

d) *If the system is able to distinguish between uses and disclosures of information, does it record a description of disclosures in a standardized manner (for example, does the system offer or require a user to select from a limited list of types of disclosures)? If yes, is such a feature being utilized and what are its benefits and drawbacks?*

Answer: For "break the glass" events, there is a limited list of selectable radio buttons from which users can select their use/purpose for requesting information (e.g., primary physician, administrative office use, etc.) We attempted to include a free-text field option to allow user- determined descriptions but these proved to be ineffective and a distraction. Users used this field to fill in information ("asdf", "other", name, etc.) they could quickly input to navigate past the attestation

screen. Radio buttons work considerably better at capturing relevant information, but are often incorrectly or randomly selected to expedite access to the patient's record.

e) *Is there a single, centralized electronic health record system? Or is it a decentralized system (e.g., different departments maintain different electronic health record systems and an accounting of disclosures for treatment, payment, and health care operations would need to be tracked for each system)?*

Answer: a. No. We have over 200 applications that use and store PHI – only our main EHR, Billing, Pharmacy, and Lab systems centrally store audit data and could be updated support AOD for TPO.

f) *Does the system automatically generate an accounting for disclosures under the current HIPAA Privacy Rule (i.e., does the system account for disclosures other than to carry out treatment, payment, and health care operations)?*

Answer: No. This is a highly manual process.

i) *If yes, what would be the additional burden to also account for disclosures to carry out treatment, payment, and health care operations? Would there be additional hardware requirements (e.g., to store such accounting information)? Would such an accounting feature impact system performance?*
ii) *If not, is there a different automated system for accounting for disclosures, and does it interface with the electronic health record system?*

Answer: NA, however, system upgrade costs and system performance impacts have been analyzed and we feel that to meet AOD suggestions for TPO, using currently available technologies, would negatively impact the speed of our EHR systems to deliver PHI to our care givers which may impact our ability to provide quality patient care. The audit logging performance costs would have to be paid by the EHR despite the fact data mining, manipulation and reporting would be done outside the EHR system. (e.g., at our enterprise data warehouse)

The HITECH Act provides that a covered entity that has acquired an electronic health record after January 1, 2009 must comply with the new accounting requirement beginning January 1, 2011 (or anytime after that date when it acquires an electronic health record), unless we extend this compliance deadline to no later than 2013.

7) *Will covered entities be able to begin accounting for disclosures through an electronic health record to carry out treatment, payment, and health care operations by January 1, 2011?*
   a) *If not, how much time would it take vendors of electronic health record systems to design and implement such a feature?*
   b) *Once such a feature is available, how much time would it take for a covered entity to install an updated electronic health record system with this feature?*

Answer: No. Current estimates are that to update our current, in house developed EHR to meet certification needs, will take at least until late 2012 or early 2013.

8) *What is the feasibility of an electronic health record module that is exclusively dedicated to accounting for disclosures (both disclosures that must be tracked for the purpose of accounting under the current HIPAA Privacy Rule and disclosures to carry out treatment, payment, and health care operations)? Would such a module work with covered entities that maintain decentralized electronic health record systems?*

Answer: This is feasible. Intermountain's EHR system currently uses a modular architecture that allows for bolt-on applications (e.g., e-Prescribing). However, we have at least 5 major systems, all running on differing database products and platforms that would need to interface to such an AOD module. In all likelihood we would need to develop a module for each of these major systems and many of the smaller applications that use and store PHI to produce the automated reporting.

9) *Is there any other information that would be helpful to the Department regarding accounting for disclosures through an electronic health record to carry out treatment, payment, and health care operations?*

Answer: Despite our considerable investment in health information technology and electronic health records, we do not now have the technological capacity to comply with the expanded accounting of disclosures requirements that newly require covered entities to, upon request, produce an accounting of disclosures report for disclosures through an electronic health record for treatment, payment and health care operations. More importantly, perhaps, we do not envision having the technological capacity to automatically generate such reports in the near-term future, even with our forthcoming $250 million investment in augmenting our health information technology capabilities over the next three years. We urge the Secretary to require that no information be recorded in accounting of disclosures reports for treatment, payment and healthcare operations until such capacity is widely available at a reasonable cost.

Our experience tells us that the additional accounting of disclosure requirements will impose massive and arduous compliance requirements on hospitals and health systems without producing any meaningful benefit sought by patients. We have had 11 requests for accounting of disclosure reports in the more than seven years since the privacy rule took effect. We do however regularly receive requests for information from patients with very specific concerns about whether a particular caregiver inappropriately accessed their record or whether inappropriate access may have occurred during a recent hospital stay. Other requests are motivated by family disputes – did my ex-husband view my record? When we receive these inquiries, we launch a privacy investigation to determine whether or not inappropriate access occurred and we discipline as appropriate.

Importantly, privacy investigations are highly manual processes. Audit logs may be tools in the investigation but they are just one component of a lengthy human review that often involves interviews, review of work records (was the nurse on duty when she accessed the information), assessment of the role in which the caregiver was working when she reviewed the record – hands-on caregiver or quality of care reviewer. Audit logs may have much data in them but the data is coded and often cryptic. Audit logs actually have little information that would easily be understandable by a patient. This is because audit logs lack context. An audit log cannot tell you whether access was appropriate or not. An audit log cannot tell you precisely what was viewed. An audit log cannot tell the difference between a use and a disclosure, etc. Our privacy investigations typically involve approximately 5-10 hours of professional time and extend up to 60 days. In our experience, patients are satisfied with the results of our privacy

investigations. This is evidenced by the low number of OCR privacy investigations conducted here at Intermountain.

Given that the definition of disclosure includes each and every access to our electronic health record by affiliated (non-employed) physicians who are authorized users of our system, the amount of information that would newly be required to be traceable under the expanded accounting of disclosure requirements would be enormous. At Intermountain, affiliated physicians constitute 75% of our doctors. Intermountain systems log 22 Million access events every month to our EHR system, which entail several hundred million audited security events. While the cost and resources that would be necessary to comply with these expanded requirements are difficult to estimate, the cost would likely run upward of $100 Million and require a significant amount of systems development work to create the tools necessary to comply with the expanded AOD reporting requirements. This additional cost would inevitably consume funds that otherwise would be spent on improving the quality of care delivered to patients.

We urge clarification with respect to the definition of "through" an electronic health record as well as a more detailed definition of an electronic health record. In our view, given that the HITECH Act defines an electronic health record as an "electronic record of health-related information on an individual that is created, gathered, managed and consulted by health care clinicians and staff," the expanded accounting of disclosures requirements should apply only to treatment, payment and health care operations disclosures from the principal clinical information system or systems, e.g., the clinical information system or systems where the majority of health-related information used by clinicians and staff are maintained. Disclosures from ancillary departmental stand-alone software systems such as those for admitting and registration, cardiology, physician transcription services etc. should not be required to be included in an accounting of disclosures report. Further, we urge consideration of limiting the universe of electronic health records for purposes of the expanded requirements to certified electronic health records for which the Secretary has adopted standards. Further clarification with respect to what constitutes a reportable disclosure would also be helpful.

We suggest and ask that disclosures between covered entities and disclosures within an Organized Health Care Arrangement be exempt from the new requirements.

We further suggest and ask that the Secretary use her discretion to delay the effective date of the expanded accounting of disclosures requirements for two years for existing and new users of electronic health records.

Thank you for the opportunity to share our concerns and comments.

Sincerely yours,

Marc Probst
Chief Information Officer, Intermountain Healthcare
Member, HIT Policy Committee

CC: Utah Congressional Delegation