

# **Discussion of AOD Certification Requirements**

**April 13, 2012**

## 2014 Edition NPRM Seeks 3 Types of Comments on AOD

Proposed language proposes to adopt AOD reporting criteria for the reporting as was articulated in 2011 Edition Certification: As an optional certification criterion.

However, public comment requested on three key items:

- *Should criteria be revised to be a mandatory certification criterion?*
- *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?*
- *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?*

# Background

## **2011 Edition included AOD as an optional certification requirement**

- “*Record treatment, payment, and health care operations disclosures.* The date, time, patient identification, user identification, and a description of the disclosure must be recorded for disclosures for treatment, payment, and health care operations, as these terms are defined at 45 CFR 164.501” (ie, [HIPAA Security Rule](#))

## **Yet, the HIPAA Security Rule specifically excludes disclosures for TPO from AOD requirements**

- “An individual has a right to receive an accounting of disclosures of protected health information made by a covered entity in the six years prior to the date on which the accounting is requested, except for disclosures: (i) To carry out treatment, payment and health care operations as provided in §164.506”
- HIPAA-required AODs thus are limited to disclosures such as research, court documents, inappropriate disclosures outside of TPO, etc

## **As a result, current AOD processes cover events that are relatively infrequent and aren’t typically recorded in EHR systems**

- Data collection is typically manual, draws from information typically held outside of the EHR, and is limited to five data fields: Date, Time, Patient ID, User ID, Description of Disclosure

## **In applying the HIPAA AOD requirement to TPO disclosures, the 2011 Edition (and proposed 2014 Edition) is thus extrapolating the HIPAA requirements to purposes for which they were not intended**

- Current HIPAA AOD requirement is functional – there is no corresponding technical specification
- Data fields required for non-TPO disclosures are assumed to be relevant to TPO disclosures

## **P&S NPRM included a number of AOD requirements related to TPO disclosures**

- The rule received considerable negative feedback during the public comment period
- Final rule has yet to be issued

# Comments

## **EHRs typically do not capture the type of information that would be required for AOD of TPO disclosures**

- HIPAA doesn't require it, and there are no technical standards
- Normal EHR audit functions do not provide information to inform “description of the disclosure”
  - Usually limited to what was read, accessed, printed, or deleted
  - Do not capture or resolve “uses” vs “disclosures” – “employed” vs “affiliated” are blurry distinctions, especially in complex AMCs/IDNs

## **Considerable groundwork would need to be laid to make AOD for TPO achievable and scalable**

- Definition of data element requirements for TPO disclosures
- Creation of technical standards for data capture and reporting
- Definition of “uses” and “disclosures” that can be clearly applied in all clinical settings
- Changes in workflow that enable capture of AOD-relevant data without unacceptably encroaching on TPO activities
  - Would require users to enter whether they are employee or affiliate, and purpose for access, for each TPO event (ie, each time they use the EHR for a care or payment event)

## Recommendations (for discussion)

***Should criteria be revised to be a mandatory certification criterion?***

- No
- Standards do not currently exist for applicability, data element requirements, technical requirements, or reporting requirements for TPO disclosures

***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?***

- Qualified yes
- As long as it does not try to add technical specifications, since the P&S Final Rule is not yet out and may address that
- However, could beg the question of how certification testing would be done

***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?***

- Given the level of feedback during the public comment period, recommend that we not try to provide this level of detail because it would take considerable time and we don't know how much of the NPRM will be retained in the final rule