Health IT Policy Committee
A Public Advisory Body on Health Information Technology to the National Coordinator for Health IT

January 22, 2014
Karen DeSalvo, MD
National Coordinator for Health Information Technology
Department of Health and Human Services
200 Independence Avenue, S.W.
Washington, DC 20201

Dear Dr. DeSalvo:

The HIT Policy Committee (Committee) gave the following broad charge to the Privacy & Security Tiger Team (Tiger Team):

Broad Charge for the Privacy & Security Tiger Team
The Tiger Team is charged with making short-term and long-term recommendations to the Health Information Technology Policy Committee (HITPC) on privacy and security policies and practices that will help build public trust in health information technology and electronic health information exchanges (HIEs), and enable their appropriate use to improve healthcare quality and efficiency, particularly as related to American Recovery and Reinvestment Act (ARRA) and the Affordable Care Act (ACA) which mandates a number of duties to the Office of the National Coordinator (ONC) relative to privacy and security.

The Privacy and Security Tiger Team was asked to provide recommendations on how to implement the requirement in the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 for covered entities and business associates to account for disclosures for treatment, payment and health care operations (TPO) made through an electronic health record (EHR). In support of this effort, the Tiger Team hosted a virtual public hearing and invited public comment through the ONC Health IT Buzz Blog. Insights from the hearing and the blog informed the Tiger Team's deliberations. This letter provides the resulting recommendations on accounting of disclosures, which were adopted by the Committee on December 4, 2013, to the National Coordinator, Department of Health and Human Services (HHS).

Background
The HIPAA Privacy Rule currently requires covered entities (CEs) to make available, upon request, an accounting of certain disclosures of an individual's protected health information (PHI) made up to six years prior to the request. The accounting should include date, name of recipient (and address, if known), a brief description of the PHI disclosed and the purpose of disclosure. The accounting requirements apply to disclosures of both paper and electronic PHI, regardless of whether such information is in a designated record set (DRS).[1] The Privacy Rule explicitly identifies a number of exemptions to the accounting requirement, including disclosures to carry out TPO.

[1] Per §164.501of HIPAA, a DRS is a group of records maintained for or by the covered entity to make decisions about the individual, such as medical bills and billing records.

The HITECH Act:

- Removed the exception for disclosures to carry out TPO for disclosures made "through an EHR."
- Reduced the time period for an accounting for disclosures report from six years to three years.
- Required CEs to provide individuals with either an accounting of disclosures of their business associates (BAs) or a list of their BAs and corresponding contact information.
- Required HHS to adopt regulations to implement these changes in a way that "takes into account the interests of the individuals in learning the circumstances under which their protected health information is being disclosed and takes into account the administrative burden of accounting for such disclosures."[2]

The HITECH Act also required the adoption of an initial set of standards, implementation specifications and certification criteria for accounting for disclosures through EHR technology.

On May 31, 2011, the HHS Office for Civil Rights (OCR) published a Notice of Proposed Rulemaking (NPRM) proposing changes to the Privacy Rule's accounting for disclosure provisions. These changes were intended to implement the HITECH changes described above and to "improve the workability and effectiveness" of the original accounting of disclosures provisions. The proposed changes to the Privacy Rule include:

- Listing the specific types of disclosures required to be included in an accounting report, such as impermissible disclosures, disclosures for public health, and other disclosures;

- Making clear that an accounting report covers those types of disclosures of an individual's protected health information (PHI) maintained in a DRS in both paper and electronic form by covered entities and BAs for three years prior to the request.

- Adding additional exceptions to the accounting requirement, such as for disclosures made for research purposes, and impermissible disclosures in which the CE (directly or through a BA) has provided breach notice.

- Modifying the content of the accounting, for example, to simplify the reporting of repeated disclosures for a single purpose by replacing multiple entries with the start and end dates of the disclosures.

To implement the HITECH changes, the NPRM proposed giving individuals a right to an "access report" that identifies all who have accessed an individual's PHI maintained in an electronic DRS by CEs and their BAs. This right would not extend to paper records. The proposed access report would include the date and time of access, name of natural person (or the entity accessing PHI if the name is not available), and a description of the information that was disclosed and the associated action (e.g., creation, modification, deletion), if available. Information that meets the definition of "Patient Safety Work Product" would be exempt from inclusion in the access report.

Regarding certification, ONC has made the ability to generate an accounting of disclosures an optional certification criterion for EHRs in its 2014 edition of the criteria; as a result, there is no requirement that

[2] HITECH Section 13405(c)(2).

Certified EHR Technology include technical capabilities to account for TPO or other disclosures.[3] ONC explained that making this criterion optional provides complete EHR and EHR module developers with the flexibility to innovate in this area and to develop new solutions to address the needs of their customers.

Virtual Public Hearing

The HITPC Privacy and Security Tiger Team hosted a virtual public hearing to discuss the NPRM, focusing in particular on the proposed approach for implementing HITECH. The hearing included witnesses grouped into four panels: Patient, Vendor/BA, Provider, and Payer (Attachment 1 contains a detailed list of witnesses). The following are key observations made during the hearing:

- Transparency to individuals about the uses and disclosures of their health information is important for building trust in health IT.
  - Such transparency should be done in a way that is understandable to individuals, including those with disabilities and those for whom English is not their primary language.
  - Patient representatives at the hearing testified that patients want the kind of transparency of record access proposed in the NPRM access report.
  - Patient representatives also emphasized the importance of their own ability to access information about them in EHRs

However:

- No testimony supported that the proposed access report was do-able, at least with current technologies. Audit trail technologies are frequently mentioned as a tool for offering greater transparency to individuals, but audit logs, when they are deployed, are designed to track security-relevant system events, not all user activity, and do not easily produce reports designed to be understandable to individuals.

- No one at the hearing offered a specific technical path forward toward accomplishing the scope of what was proposed in the NPRM access report.

- Questions were raised about the potentially significant costs to the covered entity of generating a NPRM access report.

- It's not clear that patients want, or would find value in, the deluge of information likely to be produced by the NPRM access report.
  - Today, patients rarely ask for accounting reports. Patient advocates testified that this is because the reports available today do not include much valuable information and patients are not aware of their right to ask for such a report; providers and payers testified that the historic lack of requests indicates this is not a priority for patients.
  - It seems unwise to impose a new access report mandate, given the potential costs and how little evidence we have of whether patients would ask for such reports.

- All seemed to agree that patients should have the right to a full investigation of complaints about inappropriate access; such an episodic response could be more effective at addressing patient

[3] Test Procedure for §170.314(d)(9) Optional – Accounting of disclosures

concerns versus building in expensive technology to produce a report that (1) may be less helpful in ferreting out inappropriate access (buried in reams of material) and (2) would be expensive to build for the few occasions where it is needed.

- Concerns were also raised about providing patients with the names of individual users who had accessed their health information. Neither the OECD principles, the Fair Credit Reporting Act, or the Privacy Act of 1974 provide this type of access.

- Testifiers noted that currently available technology does not distinguish between certain internal accesses and disclosures; for example, a credentialed system user may not be an employee of the organization. The HIPAA definition of disclosure also includes access by some credentialed users.

- HITECH eliminates the exemption for disclosures for treatment, payment, and health care operations (TPO), "through an EHR." Testifiers raised questions about what is meant by that term.

ONC Blog
The ONC Blog received more than a dozen comments that confirmed key points from the hearing. Major themes included:

- Views on proposed changes:

  – The proposed access report is burdensome and unlikely to provide meaningful information to patients. Commenters support a more focused approach.
  – Commenters pointed out the value of an investigation as means of addressing patient concerns about access to their information
  – There are few, if any, standard ways to generate access reports from audit logs.
  – Adding functionality to or replacing existing EHRs in order to record the purpose of access would be costly.
  – Historically, patient requests for accounting of disclosures have been limited in number.
  – There are significant safety concerns associated with releasing names of employees that have accessed a patient's record to the patient.

- Views on Patient Rights:

  – There is appreciation and support for the individual's rights associated with health information and concern over the harm caused by inappropriate access to PHI by authorized and unauthorized users alike.
  – One patient reinforced the need to make sure that it is the right of every patient to receive an accounting of disclosures
  – Patients detailed the harms that come from inappropriate use or disclosure of a patient record
  – Patients do not request an accounting because (1) it is not useful in its current form and (2) consumers have little understanding of these provisions. An incremental approach with patient education is needed.

Recommendations
Due to the uncertainties and complexities involved in implementing the HITECH requirements to account for disclosures for TPO made through an EHR (as described above), the Policy Committee recommends that HHS approach implementation in a step-wise or staged fashion, pursuing an initial

pathway that is workable from both a policy and technology perspective.

Consistent with this approach, the Policy Committee's recommendations focus on:

- The patients' rights to a report of disclosures *outside* the entity or organized health care arrangement (OHCA)[4] [5]and
- The patients' rights to an investigation of inappropriate accesses *inside* (i.e., inappropriate uses) the entity or within the OHCA.

The Policy Committee does not believe the proposed access report defined in the NPRM meets the requirements of HITECH to take into account the interests of the patient and administrative burden on CEs. Instead, the Committee urges HHS to pursue a more focused approach that prioritizes quality over quantity, where the scope of disclosures and related details to be reported to patients provide information that is useful to patients, without overwhelming them or placing undue burden on CEs. By the term "quality over quantity," the Committee means that HHS should focus, at least initially, on EHR disclosures *outside* the CE or OHCA.

To provide additional clarity on what is meant by EHR disclosures *outside* the CE or OHCA, the Committee recommends that HHS pursue a "Follow the Data" approach:

- When control of patient data is transferred to another entity, the recipient of the data should be part of an accounting of disclosures report. For example, when EHR data moves from its compliance environment to another environment, or when EHR data moves to an environment where it can be accessed by individuals who are not known to the originating EHR (e.g., persons who have not been issued credentials to access the originating EHR), these EHR data transfers are considered reportable disclosures. Attachment 2 contains additional clarifying scenarios that depict when an EHR data transfer is or is not a disclosure that would be required to be in a report to an individual at the individual's request.

- Further, individuals should also be able to obtain, upon request, an accounting of disclosures report from such recipients if the recipients are (1) BAs and (2) have further disclosed the data outside of their compliance environments, and the subsequent recipient controls and could potentially disclose the data. (Per HITECH, CEs have the option of gathering and providing this

[4] The meaning of disclosures "outside" an entity or OHCA is explained further below. The Committee does intend for these recommendations to apply to a more narrow set of information sharing than is encompassed by the definition of "disclosure."

[5] §160.103 of HIPAA defines an organized health care arrangement as: (1) A clinically integrated care setting in which individuals typically receive health care from more than one health care provider; (2) An organized system of health care in which more than one covered entity participates and in which the participating covered entities: (i) Hold themselves out to the public as participating in a joint arrangement; and (ii) Participate in joint activities that include at least one of the following: (A) Utilization review, in which health care decisions by participating covered entities are reviewed by other participating covered entities or by a third party on their behalf; (B) Quality assessment and improvement activities, in which treatment provided by participating covered entities is assessed by other participating covered entities or by a third party on their behalf; or (C) Payment activities, if the financial risk for delivering health care is shared, in part or in whole, by participating covered entities through the joint arrangement and if protected health information created or received by a covered entity is reviewed by other participating covered entities or by a third party on their behalf for the purpose of administering the sharing of financial risk. [Provisions applicable to health plans have been omitted.]

information to patients vs. the obligation being on the BA to provide information about subsequent disclosures.) [6]

In reflecting concerns raised at the public hearing and in the blog, the Committee recommends that the content of the disclosure report be required to include only an entity name rather than a specific individual as proposed in the NPRM.

Technologies to enable individuals to receive an accounting of disclosures (other than those made within an OHCA) must first be piloted by HHS before any new policies can be implemented. The Committee expressly recommends that HHS launch such pilots, and focus initially on provider EHRs. Such pilots should focus on the technical feasibility of disclosure reports, and the accompanying implementation burden on providers as well as on the feasibility and usability of such reports for patients. The content of the report should also be tested in the pilot; such testing should include the option to group similar disclosures together (vs. reporting each one individually), as permitted by the NPRM. The result of the pilot will inform regulations to implement HITECH and enable ONC to assess readiness for a future stage of EHR certification. HHS could then determine how to expand the pilot - such as to additional HIPAA covered entities or to electronic data systems that are not EHRs.

The Committee also re-emphasized the importance of the right of an individual to an investigation of alleged inappropriate access. Results of the hearing indicate that an investigation, rather than a report of access, is more likely to satisfy many patient concerns, particularly with respect to access within an organization or OHCA. Such an investigation should enable patients to ask whether a particular person (workforce member or contractor) inappropriately accessed their records or find out what happened to their records in a particular circumstance. (The Committee notes the ability of patients, under the accounting of disclosures proposed rule, to obtain a report that includes disclosures that would be considered breaches but are not required to be reported to patients.)

To improve the ability of CEs and BAs to do investigations of inappropriate access, the Committee recommends that the OCR add two implementation specifications to the current audit control standard in the HIPAA Security Rule (164.312(b)):

- (Addressable) Audit controls must record PHI-access activities to the granularity of the user (workforce member or natural person) and the individual whose PHI is accessed.
- (Addressable) Information recorded by the audit controls must be sufficient to support the information system activity review required by §164.308(a)(1)(ii)(D) and the investigation of potentially inappropriate accesses of PHI.

Given the importance of the investigations in supporting patient rights, the Committee further recommends that OCR explore whether these investigations currently are being completed and

[6] The approach taken in these recommendations is similar to the approach taken for the September 2010 "meaningful choice" recommendations: when a decision to disclose or exchange the patient's identifiable health information from the provider's record is not in the control of the provider or that provider's organized health care arrangement ("OHCA"), patients should be able to exercise *meaningful consent* to their participation). In addition, the HITPC/Tiger Team's May 2013 recommendations on query-response models, emphasized that the data holder should log a response to a query from an outside organization and that this information, along with the query, should be available to the patient upon request. In the query models studied by the Tiger Team, all involved external queries for health information.

adequately address the patient's concerns with respect to inappropriate access.

The Committee believes that these accounting of disclosures recommendations provide a solid place for HHS to start implementation of the HITECH requirements, and enables testing of both a technology and policy approach through pilots. The recommendations also provide patients with focused information to better meet their needs and are consistent with HITECH statutory language to address disclosures for TPO through an EHR while balancing the "interests of the individuals" with "administrative burden" on CEs.

We appreciate the opportunity to provide these recommendations on the accounting of disclosures and look forward to discussing next steps.

Sincerely yours,

/s/

Paul Tang
Vice Chair, HIT Policy Committee

Attachment 1: Virtual Public Hearing Witnesses
September 30, 2013

Panel I: Patient Perspectives

Mark Richert, Esq. – *Director, Public Policy*, *American Federation for the Blind*

Joanne McNabb – *Director of Privacy Education and Policy, California State and Consumer Services Agency*

Dr. Deborah Peel – *Founder, Patient Privacy Rights*

Michelle de Mooy – *Senior Associate, National Priorities, Consumer Action*

Panel 2: Vendor/Business Associate Perspectives

Kurt Long – *Chief Executive Officer and Founder, FairWarning*

Eric Cooper – *Health Information & Identity Management Product Lead, EPIC*

Jeremy Delinsky – *Chief Technology Officer, Athena Health*

John Travis – *Senior Director, Regulatory Compliance*

Lori Cross – *Director of Laboratory Operations, Cerner*

Panel 3: Provider Perspectives

Darren Lacey – *Chief Information Security Officer, Johns Hopkins University Health System*

Lynne Thomas Gordon – *Chief Executive Officer, American Health Information Management Association*

Jutta Williams – *Director, Corporate Compliance Privacy Office, Intermountain Healthcare*

William Henderson – *Administrator, The Neurology Group, LLP (Albany, NY) and Co-Chair, Board of Directors of Medical Group Management Association*

Kevin Nicholson – *Vice President, Public Policy and Regulatory Affairs, National Association of Chain Drug Stores*

Panel 4: Payer Perspectives

Scott Morgan – *Executive Director, National Privacy and Security Compliance Officer, Kaiser Permanente*

Jay Schwitzgebel – *Director Information Security & IT Compliance, Caresource*

Attachment 2: Illustrative Scenarios for the Accounting of Disclosures Recommendation

As discussed above, the Policy Committee recommends that HHS pursue a "Follow the Data" approach for the accounting of disclosures requirement. Specifically, when EHR data moves from its compliance environment to another environment or when EHR data moves to an environment where it can be accessed by individuals who are not known to the originating EHR, these EHR data transfers are considered "accountable" disclosures. The following are illustrative scenarios of disclosures that would trigger an entry into the accounting of disclosures report:

- Data is moved from a provider to an HIE, where access, use and disclosure are determined by HIE policy.
- Data is sent to an entity to facilitate e-prescribing.
- Data is sent to a health plan for payment, or to an external provider for treatment.
- Data is sent to a registry for quality improvement.
- Data is disclosed pursuant to Meaningful Use Stage 2 information exchange requirements (for example, using Direct to transmit a Continuity of Care Document (CCD) to another facility).
- Data is moved from a provider to a recipient who has the independent ability, for example to:
  - Resell or otherwise monetize the data
  - Disclose the data to other covered entities
  - Use the data for internal purposes other than quality review
  - Create a Limited Data Set (LDS) or de-identify the data for purposes unrelated to the covered entity

The following are illustrative scenarios of disclosures that would not trigger an entry in the accounting of disclosures report:

- Access to a hospital EHR by a community physician using his/her security credentials (for example, user name & password)
- Automatic or manual transfers of information from an EHR to other electronic systems within the entity or OHCA