Health IT Policy Committee

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

Privacy & Security Tiger Team: Accounting of Disclosures Recommendations

December 4, 2013

Tiger Team Members

- **Deven McGraw, Chair,** Center for Democracy & Technology
- **Paul Egerman, Co-Chair,** Entrepreneur
- **Dixie Baker,** Martin, Blanck, and Associates
- **Judy Faulkner,** Epic Systems Corporation
- **Leslie Francis,** University of Utah College of Law
- **Larry Garber**, MD, Reliant Medical Group
- **Gayle Harrell,** Consumer Representative/Florida
- **John Houston,** University of Pittsburgh Medical Center
- **David McCallie,** Cerner Corporation
- **Wes Rishel,** Gartner
- **Micky Tripathi,** Massachusetts eHealth Collaborative
- **Kitt Winter,** Social Security Administration

Agenda/Roadmap

- Present recommendations on Accounting of Disclosures to the HITPC
  - Background
    - Current regulatory requirements
    - HITECH requirements
    - OCR Notice of Proposed Rulemaking (NPRM)
  - Key Points: September 30th hearing
  - Summary of public comments submitted through Health IT Buzz Blog
  - Recommendations:
    - Patient's right to a report of disclosures *outside* the entity or Organized Health Care Arrangement (OHCA)
    - Patient's right to an investigation of accesses *inside* the entity

Current Regulatory Requirements (1 of 2)

- HIPAA Privacy Rule currently requires covered entities to make available, upon request, an accounting of certain disclosures of an individual's PHI made up to six years prior to the request.
  - Accounting should include date, name of recipient (and address, if known), brief description of the PHI disclosed and purpose of disclosure.
  - Privacy Rule accounting requirements apply to disclosures of both paper and electronic PHI, regardless of whether such information is in a designated record set (DRS).
  - 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.

Current Regulatory Requirements (2 of 2)

- Exceptions include the following disclosures:
  - To carry out treatment, payment or operations (TPO).
  - To the individual who is the subject of the PHI.
  - Made under an authorization.
  - As part of a limited data set under a data use agreement.
  - Made prior to the compliance date.
  - For the facility's directory or persons involved in the individual's care.
  - For national security or intelligence purposes.
  - Incident to a permissible use or disclosure.
  - To correctional institutions or law enforcement officials.

HITECH Requirements

- The HITECH Act requires new rulemaking to implement changes to the Accounting of Disclosures requirements:
  - The exception for disclosures to carry out TPO would no longer apply if made through an EHR.
  - Individuals would have a right to receive an accounting of disclosures made during the three years prior to the request, as opposed to six.
  - Covered entities would be required to provide either an accounting of a business associate's disclosures or a list and contact information of all business associates to the individual requesting the accounting.
- The HITECH Act also requires the adoption of an initial set of standards, implementation specifications and certification criteria for accounting of disclosures in EHR technology.

OCR NPRM (1 of 6)

- After receiving responses to an RFI published on May 3, 2010, the HHS Office for Civil Rights (OCR) released an NPRM to change the Privacy Rule's Accounting of Disclosures requirements.
- NPRM would provide individuals with two rights:
  - An accounting of disclosures and
  - An "access report".

OCR NPRM (2 of 6)

- An accounting of the following disclosures made of an individual's PHI maintained in a designated record set (DRS) in both paper and electronic form by covered entities and business associates:
  - Impermissible disclosures and disclosures for public health, judicial and administrative proceedings, law enforcement activities, military and veterans activities, situations to avert a serious threat to health or safety, State Department medical suitability determination, government programs providing public benefits, and workers' compensation.

OCR NPRM (3 of 6)

- Proposed exceptions in addition to the existing exceptions* in the Privacy Rule:
  - In the case of abuse, neglect or domestic violence.
  - For research purposes, where an Institutional Review Board (IRB) waives authorization.
  - Impermissible disclosures in which the covered entity (directly or through a business associate) has provided breach notice.
  - Disclosures required by law.
  - For health oversight purposes.
  - About decedents to coroners and medical examiners.
  - For information that meets the definition of "Patient Safety Work Product," which would fall under the privilege and confidentiality provisions of the Patient Safety and Quality Improvement Act of 2005.

*For existing exceptions, see slide #5.

OCR NPRM (4 of 6)

- The NPRM proposes to require the content of the accounting to include:
  - The date, if known; or if not, the approximate date or period of time during which the disclosure occurred;
  - The name of the entity or natural person* who received the protected health information and, if known, the address of such entity or person, except when such information constitutes protected health information about another individual;
  - A brief description of the type of protected health information disclosed; and
  - A brief description of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure.

*A natural person is a real human being, as opposed to a legal person, which may be a private (business) entity or public (government) organization.

OCR NPRM (5 of 6)

- Right to an "access report" that indicates who accessed an individual's PHI maintained in an electronic DRS. This right does not extend to paper records. Proposed rule requires revisions to Notice of Privacy Practices to inform individuals about their right to an access report. Must contain the following:
  - Date and time of access
  - Name of natural person,* if available, otherwise the entity accessing PHI
  - Description of information disclosed and user action (creation, modification, deletion), if available.
  - The NPRM notes that an electronic DRS system may exchange data with another electronic system within the organization. In such cases, the access report can identify such access by the name of the covered entity in order to reflect that the individual's information was accessed by one of the covered entity's systems.

*A natural person is a real human being, as opposed to a legal person, which may be a private (business) entity or public (government) organization.

OCR NPRM (6 of 6)

- A proposed exception to the access report would be for information that meets the definition of "Patient Safety Work Product," which would fall under the privilege and confidentiality provisions of the Patient Safety and Quality Improvement Act of 2005.

EHR Certification

- Regarding certification, ONC has made accounting of disclosures an optional certification criteria for EHRs in its 2014 edition of the criteria.
- Intention is to leave 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. Certification capability will not be required**.

**Test Procedure for §170.314(d)(9) Optional – Accounting of disclosures

Key Hearing Points (1 of 5)

- 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 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 access to information about them in EHRs

Key Hearing Points (2 of 5)

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 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 of the NPRM access report.

Key Hearing Points (3 of 5)

- 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.

Key Hearing Points (4 of 5)

- 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 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. Questions were raised about whether the OECD principles, the Fair Credit Reporting Act, or the Privacy Act of 1974 provide this type of access

Key Hearing Points (5 of 5)

- Testifiers noted that technology does not distinguish between an internal access and a disclosure; 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.

Key Points from Public Comments (1 of 2)

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.

Key Points from Public Comments (2 of 2)

- **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 Overview

The Tiger Team is making recommendations on how to implement the HITECH requirement to account for disclosures for TPO made through an EHR. The recommendations focus on:

- The patient's right to a report of disclosures *outside* the entity or OHCA
- The patient's right to an investigation of accesses *inside* the entity

Recommendations: Right to a Report of External Disclosures (1 of 7)

- Given the uncertainties and complexities involved in implementing the HITECH requirements, HHS should approach this in a step-wise fashion, initially pursuing an implementation pathway that is workable from both a policy and technology perspective.
- The Tiger Team does not believe the proposed access report meets the requirements of HITECH to take into account the interests of the patient and administrative burden on covered entities (CEs).
- Instead, we urge 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.

Recommendations: Right to a Report of External Disclosures (2 of 7)

"Quality over quantity" means that:

- In responding to the HITECH requirement to account for disclosures for TPO, HHS should focus, at least initially, on EHR disclosures *outside* the CE or OHCA

Recommendations: Right to a Report of External Disclosures (3 of 7)

- HHS should 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.
    - Additional ways to conceive of this:
      - EHR data moves from its compliance environment to another environment, where it can be further accessed and/or disclosed.
      - EHR data is moved to an environment where it can be accessed by individuals not known to the originating EHR.
  - Patients should also be able to obtain an Accounting of Disclosures report from such recipients if they are (1) business associates 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, covered entities have the option of gathering and providing this information to patients vs. the obligation being on the business associate to provide information about subsequent disclosures.)

Illustrative Scenarios Triggering Report (1 of 2)

- 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 CCD to another facility).

Illustrative Scenarios Triggering Report (2 of 2)

- 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

Illustrative Scenarios NOT Triggering 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

Recommendations: Right to a Report of External Disclosures (4 of 7)

- Technologies and policies to accomplish this should first be piloted by ONC
  - Focus first on provider EHRs per HITECH; after pilots and initial implementation, HHS could then determine how to expand (such as to additional HIPAA covered entities or to electronic data systems that are not EHRs)
  - Pilots should focus on technical feasibility of disclosure reports, as well as on feasibility and usability of such reports for patients and implementation burden on providers.
  - Pilots will enable ONC to assess readiness for a future stage of EHR certification.

Recommendations: Right to a Report of External Disclosures (5 of 7)

Regarding content of the report:

- The accounting of disclosures should require only an entity name rather than the specific individual as proposed
  - Testifiers at the hearing stated that this proposed requirement may subject employees to privacy intrusions and create safety concerns
- Content of the report should be tested in the pilot; such testing should include the possibility to group similar disclosures together (vs. reporting individually), as permitted by the proposed Accounting of Disclosure rule.

Recommendations: Right to an Investigation (6 of 7)

- The Tiger Team also reinforces 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 an accounting, may satisfy many patient concerns
  - Such an investigation should enable patients to ask whether a particular individual inappropriately accessed their records or find out what happened to their records in a particular circumstance.
  - The Tiger Team 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

Recommendations: Right to an Investigation (7 of 7)

- To improve the ability of covered entities to do investigations of inappropriate access, the Tiger Team recommends that the Office for Civil Rights add two implementation specifications to the current audit control standard in the HIPAA Security Rule (164.312(b)):

  1) (Addressable) Audit controls must record PHI-access activities to the granularity of the individual user (i.e., human) and the individual whose PHI is accessed.

  2) (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 potential inappropriate accesses of PHI.

*164.308(a)(1)(ii)(D) requires implementation of "procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports." 164.312(b) sets an audit control standard that requires implementation of "hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information."

Rationale for Recommendations (1 of 2)

- Provides a solid place for HHS to start implementation, and enables testing of both technology and policy approach through pilots
- Provides patients with focused information to better meet their needs, i.e., quality over quantity
- Consistent with HITECH statutory language
  - Addresses disclosures for TPO through an EHR
  - Balances the "interests of the individuals" with "administrative burden"

Rationale for Recommendations (2 of 2)

- Consistent with prior Tiger Team work
  - Similar to approach taken to "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). (See backup slide 38)
  - Focus on actual disclosures also part of query recommendations. (see backup slide 36)

Accounting of Disclosures Recommendations

BACKUP

Example of Previous Recommendation re: Patient Access (August 2013)

- Patient Access to Information in EHR Systems: Eligible Providers (EPs) and hospitals should deploy audit trails for a patient's portal, and at least be able to provide these to patients upon request. Audit trail capability for the portal will need to be part of Stage 2 certification requirements.
- The ONC Final Rule (2014 edition) for the EHR certification program requires that certified EHRs be capable of (1) recording an activity history log, which monitors when electronic health information is viewed, downloaded or transmitted to a third party and (2) making this log available to the patient.

Query and Response recommendations: Approved at the April 4, 2013 HITPC meeting (Scenarios 1 and 2) and the August 7, 2013 meeting (Scenario 3). Transmittal letter sent August 23, 2013.
http://www.healthit.gov/facas/sites/faca/files/HITPC_Transmittal_08212013.pdf

Example of Previous Recommendation re: Patient Access (May 2013)

Regarding targeted query for direct treatment under HIPAA, should there be a requirement to account for and log query and/or disclosures, and should the log be shared with the patient upon request?

- Yes. The data holder should log both the query from an outside organization and the response, regardless of its content. The requester should also log the query. This information should be available to the patient upon request.

Note: Patient Access to Information in EHR Systems: Approved at the January 8, 2013 HITPC meeting. Transmittal letter sent May 3, 2013. http://www.healthit.gov/sites/default/files/hitpc_transmittal_050313_pstt_recommendations.pdf

Core Values (September 2010)

- The relationship between the patient and his or her health care provider is the foundation for trust in health information exchange, particularly with respect to protecting the confidentiality of personal health information.
- As key agents of trust for patients, providers are responsible for maintaining the privacy and security of their patients' records.
- We must consider patient needs and expectations. Patients should not be surprised about or harmed by collections, uses, or disclosures of their information.
- Ultimately, to be successful in the use of health information exchange to improve health and health care, we need to earn the trust of both consumers and physicians.

Context for Meaningful Choice Recommendations (September 2010)

- When the 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.
- The Tiger Team had concluded that such disclosures heighten privacy concerns.

*See following slide for definition.
Note: Meaningful Choice recommendations: Approved at the August 19, 2010 HITPC meeting. Transmittal letter sent September 9, 2013. http://www.healthit.gov/sites/default/files/hitpc_transmittal_p_s_tt_9_1_10_0.pdf

Organized Health Care Arrangement: Definition

Organized health care arrangement (45 CFR 160.103) means:

(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 omitted]