Health IT Policy Committee

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

HIT Policy Committee Privacy & Security Tiger Team Virtual Hearing on Accounting for Disclosures

Monday, September 30, 2013

11:45am ET

Agenda

1. **Call to Order/Roll Call**
   - ***Michelle Consolazio, Office of the National Coordinator for Health IT***
2. Opening Remarks/Framing & Introductions
3. Panel I: Patient Perspectives
4. Question and Answer
5. Panel 2: Vendor/Business Associate Perspectives
6. Question and Answer
7. Panel 3: Provider Perspectives
8. Question and Answer
9. Panel 4: Payer Perspectives
10. Question and Answer
11. Wrap Up/Next Steps/Closing Remarks
12. Public Comment
13. Adjourn

Health IT Policy Committee

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

Virtual Hearing on Accounting of Disclosures

September 30, 2013

11:45am to 5:00pm

Purpose

- Explore realistic ways to provide patients with greater transparency about the uses and disclosures of their digital, identifiable health information. Such exploration should also help facilitate implementation of the HITECH requirement that a patient's right under the HIPAA Privacy Rule to an "accounting" of disclosures include disclosures for "treatment, payment and operations" when such disclosures are made through "an electronic health record."

Goals

Gain a greater understanding of :

1) **What patients would like to know about uses and disclosures of their electronic protected health information (PHI).**
2) **The capabilities of currently available, affordable technology that could be leveraged to provide patients with greater transparency re: access to/disclosure of PHI.**
3) **How record access transparency technologies are currently being deployed by health care providers, health plans, and their business associates (for example, HIEs).**
4) **Other issues raised as part of the initial proposed rule to implement HITECH changes to the current HIPAA Privacy Rule accounting of disclosures requirements.**
5) **The difficulty in making the distinction between "uses" and "disclosures".**

Regulatory Background

- HIPAA Privacy Rule 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.

Regulatory Background

- 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 disclosures.
  - To correctional institutions or law enforcement officials.

Regulatory Background

- The HITECH Act requires new rulemaking to implement these changes to the Accounting of Disclosures requirements:
  - The exemption for disclosures to carry out TPO would no longer applies 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 Notice of Proposed Rulemaking (NPRM)

- 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 Notice of Proposed Rulemaking (NPRM)

- An accounting of disclosures made of an individual's PHI maintained in a DRS in both paper and electronic form by covered entities and business associates. The NPRM provides a list of disclosures to be included in the accounting.
  - These include 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.

- Proposed exceptions to the accounting of disclosures are as follows. These are 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. The covered entity is not required to account for such disclosures.
  - 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. This exclusion also applies to access reports.

OCR Notice of Proposed Rulemaking (NPRM)

- 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 person or entity accessing PHI
  - Description of information and user action (creation, modification, deletion).
- 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.

HIPAA Omnibus Rule and Certification

- OCR did not address accounting of disclosures in the final HIPAA Omnibus Rule, issued in January 2013.
- 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

Agenda

11:45 a.m.	**Welcome and Roll Call** *Michelle Consolazio, Office of the National Coordinator for Health IT*
11:50 a.m.	**Opening Remarks/Framing & Introductions** *Deven McGraw, Chair* *Paul Egerman, Co-Chair* *Linda Sanches, Office for Civil Rights*
12:05 p.m.	**Panel I: Patient Perspectives** Mark Richert, Esq. - Director, Public Policy *-American Federation for the Blind* Dr. Deborah Peel – Founder *-Patient Privacy Rights* Michelle de Mooy – Senior Associate, National Priorities *-Consumer Action*
12:20 p.m.	**Question and Answer**

Agenda (cont.)

1:10 p.m.	**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 Stephanie Zaremba – Senior Manager, Government and Regulatory Affairs *-Athena Health*
	John Travis - Senior Director, Regulatory Compliance Lori Cross - Director of Laboratory Operations *-Cerner*
1:30 p.m.	**Questions and Answer**

Agenda (cont.)

2:30 p.m.	**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 and Chief Privacy Officer *-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*
2:55 p.m.	**Question and Answer**

Agenda (cont.)

3:50 p.m.	**Panel 4: Payer Perspectives**
	Scott Morgan – Executive Director, National Privacy and Security Compliance Officer *-Kaiser Permanente*
	Jay Schwitzgebel – Director Information Security & IT Compliance *-Caresource*
4:00 p.m.	**Question and Answer**
4:40 p.m.	**Wrap up/Next Steps/Closing Remarks**
4:45 p.m.	**Public Comment**
5:00 p.m.	**Adjourn**

Patient Panel

Mark Richert, Esq.

Director, Public Policy

American Federation for the Blind

Patient Panel

Joanne McNabb

Director of Privacy Education and Policy

California State and Consumer Services Agency

Patient Panel

Dr. Deborah Peel

Founder

Patient Privacy Rights

Michelle de Mooy

Senior Associate, National Priorities

Consumer Action

Question & Answer

Vendors/Business Associates Panel

Kurt Long

Chief Executive Officer and Founder

FairWarning

Vendors/Business Associates Panel

Eric Cooper

Health Information & Identity Management Product Lead

Epic

Vendors/Business Associates Panel

Jeremy Delinsky

Chief Technology Officer

Stephanie Zaremba

Senior Manager of Government and Regulatory Affairs

Athena Health

Vendors/Business Associates Panel

John Travis
Senior Director, Regulatory Compliance

Lori Cross
Director of Laboratory Operations

Cerner

Accounting of Disclosures Hearing – 09/30/13 HIT Policy Committee Privacy and Security Tiger Team

John Travis

Senior Director
Regulatory & Compliance Strategy
Cerner

Perspective of Our Testimony

- **Ancillary Information Systems such as a LIS or a RIS**
  - May operate standalone interfaced or as integrated with other clinical systems within a hospital or large ambulatory clinic/practice environment
  - May operate as the main clinical system in standalone provider environment like a reference lab or diagnostic imaging center
  - By volume – lab data may be as much as 70% of the medical record and 90% of the operations (or accesses) within the lab are by automated devices in some way
  - Every Radiology order involves an automated device
- **We will reflect on the abilities of the current state portfolio of both legacy systems and newer products**
- **We focused on mainly on questions found under Goal 2 from the list provided most applicable to vendors**
- **We assume the term "access" to mean any online access by natural person or machine to ePHI**
  - We view the terms "use" and "disclosure" to have the meanings defined by HIPAA when applied to access to ePHI

Cerner

Goal 2, Question 1 – Current Capabilities to Track/Monitor Access or Disclosure of PHI

- **Keep in mind RIS or LIS may be in a contributing role or may be the main clinical system in use**
- **Several typical candidate log sources for disclosure or access**
  - Distribution logs of diagnostic test reports
    - *Generated from operations jobs*
    - *Would include meta data about the disclosure as to when, by whom (at entity level), to whom, of what to a degree (report format)*
    - *Implied as why to be treatment*
    - *Shorter term retention*
  - Security Audit Logs
    - *May exist along side or within clinical system*
    - *Would include meta data about when, by whom, of what, using what and from where as to meta data about the access*
    - *Implied as to why by other meta data*
    - *Likely not containing to whom*
    - *Longer term retention*

Goal 2, Question 1 – Current Capabilities to Track/Monitor Access or Disclosure of PHI

- **Several Log Sources – Access or Disclosure**
  - Interface transaction logs
    - *Exchange with medical device, instrumentation or other applications*
    - *May be full transaction*
    - *Short retention*
  - Public health submission logs and files
    - *Submission event logs or records*
    - *Batch files*
- **Aside from security audit logs**
  - Other log sources likely do not provide patient specific reporting even though they may have patient specific information in them
  - All would require some manner of extracting of data if to be used
  - Most would not be logs of natural person/user accesses but machine processes or automated operations

Cerner

Goal 2/Question 2 – Means to Distinguish Internal User from External Disclosure

- **Possible Available means**
  - User ID or Name
  - User Roles
  - Secondary Metadata about access that establish where (Machine or IP Address, Facility Affiliation, User Location)
- **Limitations**
  - User ID/Name or Role utility depends on conventions used in implementation
    - *A contractor can act in same healthcare role as an employee, may be on site using same access devices with similar privileges as an employee*
    - *Differentiation between employee and contractor/business associate depends on implementer having ascribed meaning to user id/name or role to support that purpose*
  - Secondary meta data bears no guarantee of supporting it given employees and contractors may be working side by side even in similar labor roles
  - Determining an access to be "improper" in a patient's eyes may require more context than is afforded by user ID/name or role
    - *Context may require a combination of meta data with user identity and role to help distinguish use from disclosure*
  - Also must factor in external business associate systems like an independent reference lab doing some testing on behalf of a hospital lab

Goal 2/Question 5 – Uses, Accesses or Disclosures That Do Not Raise Privacy Concerns

- **In NPRM, OCR included possibility of system to system or server to server machine operations or accesses be included**
- **Depending on how this is interpreted,**
  - System to system might be application to application for internal interfacing within an entity
    - *Outbound result interfacing from an ancillary system*
  - Might include system to medical device or instrumentation as would be true of ancillary system
  - Taken to extreme, volume could be numbing with little added value
- **If goal is to hold provider accountable about internal propagation of ePHI**
  - Natural human/end user accesses can account for that
  - OCR could include identifying the system where the access occurred in access report requirements if the concern is “where did my data go”

Cerner

Goal 2/Question 6 – Logging Retention and Reporting

- **Reflecting back on the kinds of logs identified in response to Goal 2/Question 1**
  - Security audit logs meet retention and reporting needs including export of data from an ancillary perspective to contribute to a consolidated reporting to the patient
  - Other kinds of logs all bear several needs to be usable
    - *Require some kind of data extraction*
    - *Require some kind of retention outside the source logging mechanism*
    - *Require post processing to make use of the data as to making it "patient friendly" and normalized*
    - *Rely on other reporting and/or extraction mechanisms to provide patient specific context whether to contribute data only about a given patient asking for the reporting or to contribute log data as a matter of routine to a centralized logging or reporting function*
  - Very difficult historically for accounting of disclosures to cost justify a central repository continuously maintained to respond to low volume of requests
    - *Same issue presents itself for the access report*
    - *Made more challenging if considering machine accesses*
    - *Devices may have very limited ability to know of inquiries*

Cerner

Goal 4/Question 3 – Concerns with Disclosing Names of Individuals Accessing ePHI

- **Aside from sensitivity about disclosing individuals, practical issues of doing so include**
  - Normalizing user name/identity references across all log sources
  - Identifying the purpose of the access in a patient understandable manner across all log sources when it is often implied
    - *Issues with normalizing meaning of system operations between systems*
    - *Issues with assuring integrity of chronology of events if source systems not all using trusted external time synchronization*
  - Distinguishing for the patient what is perfectly normal from what may be abnormal patterns of access based on what can be had from source data

Cerner

Key Summary Points

- **Ancillary systems have multiple log sources possible**
  - Aside from security audit, others focused on clinical result distribution, interfacing and public health reporting may be important for disclosure activity
- **Ancillary systems may have unique definitions and meanings to user IDs/names/roles, and events/operations that would need to be normalized to be useful for consolidated reporting at a covered entity/OHCA level**
  - Consideration also needs to be given to business associates who provide diagnostic testing like reference labs as they would be potentially in scope for the access report/accounting of disclosures
- **Availability of log data for consolidation may require significant custom programming and extraction**
  - Post processing of data will be required
- **Ancillary systems also often may be the main clinical system in certain kinds of provider settings**
- **Informing the patient of machine operations may offer little additional value, be numbing in volume and hard to understand**
- **Best practice guidance on how to consolidate disparate log data for usernames/IDs, security roles, event/operation performed and dealing with implied purpose of access would be helpful**

Recommendations

- **We suggest strong consideration be given to addressing how best to constructively help the patient understand what they may be receiving should they ask for an access report**
  - Flexibility in reporting and meeting requirements – For example, can reporting be collapsed down to show one row for a unique user acting in a unique role on a specific date who accessed the ePHI?
  - Can best practice guidance be developed to help get at the patient's root interest in asking for the report without getting a "patient friendly" data dump?
  - Can best practice guidance be developed to help normalize key meta data required for the access report and accounting of disclosures across systems or to use within legacy systems?
  - Are additional data columns such as user relationship to the patient, source system and device/point of access needed to help establish context?

Questions?

John Travis
Senior Director
Regulatory & Compliance Strategy
Email: john@cerner.com
Phone: (816) 201-1465

Question & Answer

Provider Panel

Darren Lacey

Chief Information Security Officer

Johns Hopkins University Health System

Provider Panel

Lynne Thomas Gordon

Chief Executive Officer

American Health Information Management Association

Provider Panel

Jutta Williams

Director, Corporate Compliance Privacy Office and Chief Privacy Officer

Intermountain Healthcare

Provider Panel

William Henderson

Administrator, *The Neurology Group, LLP (Albany, NY)*

Co-Chair, *Board of Directors of Medical Group Management Association*

Provider Panel

Kevin Nicholson

Vice President, Public Policy and Regulatory Affairs

National Association of Chain Drug Stores

Question & Answer

Scott Morgan

Executive Director, National Privacy and Security Compliance Officer

Kaiser Permanente

Jay Schwitzgebel

Director Information Security & IT Compliance

Caresource

Question & Answer

Public Comment

Thank you and thank you to all of our distinguished panelists.

BACKUP SLIDES

Questions

Goal 1: Gain a greater understanding of what patients would like to know about uses, accesses, and disclosures of their electronic protected health information (PHI).

1) What are the reasons patients may want to learn who/what entities have used, accessed or received their PHI as a disclosure? What are the reasons they might want to know about internal uses or accesses?
2) What information would patients want to know about such use, access, or disclosure?
3) For example, is it important to know the purpose of each, or the name or role of the individual involved?
4) What are acceptable options for making this information available to patients? (report, investigation, etc.)
5) If there are limitations to the information about uses, accesses or disclosures that can be automatically collected given today's technologies, what are the top priorities for patients?
6) If patients have a concern about possible inappropriate access to or disclosure of their health information, what options currently are available to address this concern? What options should be developed for addressing or alleviating that concern?

Questions

Goal 2: Gain a greater understanding of the capabilities of currently available, affordable technology that could be leveraged to provide patients with greater transparency re: use, access, or disclosure of PHI.

1) What capabilities are currently used to enable transparency regarding (or to track or monitor) each use, access, or disclosure of PHI? To whom (and for what purpose) is this information communicated?
2) If you currently do not track each user that accesses a record internally along with the purpose of that access, what would it take to add that capability from a technical, operational/workflow, and cost perspective? What would it take to add that capability for external disclosures?
3) Is there is any "user role" or other vehicle that can be utilized to distinguish an access by in internal user from an external disclosure? Can it be determined, for example, that the user is a community physician who is not an employee of the healthcare organization (IDN or OHCA)? If not, what are the obstacles to adding this capability?
4) Does the technology have the capability to track access, use, or disclosure by vendor employees, like systems' administrators, (for example, who may need to occasionally access data in native mode to perform maintenance functions) ? Do you currently deploy this capability and if so, how?
5) Are there certain uses, access, or disclosures within a healthcare entity that do not raise privacy concerns with patients? What are these uses and disclosures? Can the technology distinguish between these others that might require transparency to patients?
6) Do you have the capability to generate reports of access to, uses of, and disclosures from, a medical record?
    - How frequently are the reports generated, and what do they look like?
    - How granular are these reports? Are they detailed by aggregate data categories, individual type of data, or individual data element, or in some other way?
    - Can they be generated automatically, or do you use manual processes?
    - Do you integrate reports across multiple systems?
    - What is the look-back period?

Questions

Goal 3: Gain a greater understanding of how record access transparency technologies are currently being deployed by health care providers, health plans, and their business associates (for example, HIEs).

1) How do you respond today to patients who have questions or concerns about record use/access/disclosure? What types of tools/processes would help you improve your ability to meet patient needs for transparency regarding record use/access/disclosure? Have you ever received a request from a patient (or subscriber) that requested a list of every employee who had access to PHI?
2) What types of record use/access/disclosure transparency or tracking technologies are you deploying now and how are you using them?
3) For transparency, what do you currently provide to patients regarding use/access and disclosure, and do you see any need to change your current approach?
4) Do you have any mechanisms by which patients can request limits on access? For example, if a patient had concerns about the possibility that a neighbor employed by the facility might access his/her record, is there a way for this to be flagged?

Questions

Goal 4: Gain a greater understanding of other issues raised as part of the initial proposed rule to implement HITECH changes.

1) Regarding access reports, what information do you collect besides the basic information collected in an audit log?
2) What would be involved in obtaining access information from business associates? Do current business associate agreements provide for timely reporting of accesses to you or would these agreements need to be renegotiated?
3) What issues, if any, are raised by the NPRM requirement to disclose the names of individuals who have accessed/received copies of a patient's PHI (either as part of a report of access/disclosures or in response to a question about whether a specific person has accessed)? What are the pros and cons of this approach?
4) How do you think current mechanisms to allow patients to file a complaint and request an investigation regarding possible inappropriate uses or disclosures are working? Could they be enhanced and be used in lieu of, or in addition to receiving a report?
    - Should entities be required to do such an investigation – if so, what should be the scope?
    - Should entities still be required to produce a report if the patient wants one?
    - What recourse does the patient have if he/she is not satisfied with the response?
    - What options do entities have if patient's transparency requests cannot be honored?