Testimony of

Lynne Thomas Gordon, MBA, RHIA, CAE, FACHE, FAHIMA
Chief Executive Officer
American Health Information Management Association

to the
US Department of Health and Human Services
Office of the National Coordinator
Health Information Technology Policy Committee Privacy and Security Tiger Team

Virtual Hearing on Accounting of Disclosures

September 30, 2013

Good afternoon. Ms. McGraw, Mr. Egerman, and members of the Tiger Team, thank you for inviting AHIMA to testify today "to explore realistic ways to provide patients with greater transparency about the uses and disclosures of their digital, identifiable health information."[1]

My name is Lynne Thomas Gordon and I am the Chief Executive Officer of the American Health Information Management Association (AHIMA). Prior to joining the AHIMA team, I served as the associate vice president for hospital operations at Children's Hospital at Rush University Medical Center in Chicago, Illinois.

AHIMA is an 85-year-old not-for-profit association of professionals, educated, trained, certified and working in the field of health information management (HIM). We have more than 67,000 members who work in multiple settings including hospitals, physician offices, long term care organizations, clinics, colleges and universities, health information technology vendors and developers, consulting firms and life science companies across the healthcare industry. AHIMA's members can be found in numerous and diverse roles with a wide range of responsibilities. Individual members are educators; hospital administrators; deans of universities; lawyers; students pursuing advanced degrees and careers in informatics; government officials; coders and data analysts, and consultants and industry professionals.

AHIMA members are subject matter experts and AHIMA is an unbiased, trusted authoritative source within the health information management and applied informatics communities. AHIMA and its members are ensuring quality health and healthcare through data and information governance and stewardship.

AHIMA provides certification in a number of practice areas, including:

- Health Information Management
    - Registered Health Information Administrator (RHIA)
    - Registered Health Information Technician (RHIT)
- Coding
    - Certified Coding Associate (CCA)
    - Clinical Coding Specialist (CCS)
    - Clinical Coding Specialist-Physician Based (CCS-P)
- Specialty
    - Clinical Documentation Improvement Practitioner (CDIP)
    - Certified Health Data Analyst (CHDA)
    - Certified in Healthcare Privacy and Security (CHPS)
    - Certified Healthcare Technology Specialist (CHTS)

[1] Rehman, Omar. Privacy and Security Tiger Team Hearing Invitation Letter. September 2013.

For more than 85 years AHIMA's members have been on the front lines and in the trenches of health information management practice, especially privacy and security requirements and adherence to the applicable federal and state laws. AHIMA members are committed to several foundational principles and tenets, especially data integrity and data confidentiality. These principles are the basis for our comments today.

AHIMA's oral testimony focused on two primary topics:

1. Data Collection, Management and Processing--Ensuring Balance
2. Ensuring the Safety of the Healthcare Workforce

Our written testimony will focus on the questions supplied by the Privacy and Security Tiger Team.

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?*

Our members report that patients rarely request specific data about *who or what entities have used, accessed or received their PHI*, especially with regard to internal uses or accesses. When an accounting of disclosure is requested, it is usually for a very specific disclosure that the patient is already aware of but would like to learn more about.

AHIMA members have indicated that the primary reason patients request an access or disclosure report is that the patient suspects that a particular party(s) may have inappropriately accessed, used, or disclosed their PHI. For example, a patient may want to know:

- Whether a former or current acquaintance has been looking at his or her record for some inappropriate purpose.
- To see if relatives or friends who work in the hospital or provider's office have accessed their medical record.
- To learn the names of the staff/physicians who accessed their record and provide this information to an attorney to subpoena them.
- Whether a sibling has accessed information on a parent or a deceased parent in an effort to resolve family matters such as settling estates.
- Employees of covered entities may be "required" by their insurance to obtain treatment at the organizations at which they work, and the employee may want to know if co-workers (not their caregivers) have been inappropriately accessing their records.

2. *What information would patients want to know about such use, access, or disclosure? For example, is it important to know the purpose of each, or the name or role of the individual involved?*

AHIMA's members report that patients typically seek to confirm any instances of inappropriate access. The patients often seem to have an awareness of who may have inappropriately accessed their data and when the access may have occurred. Our members report that patients do not seem to question routine use or access by individuals performing their jobs.

3. *What are acceptable options for making this information available to patients? (report, investigation, etc.)*

AHIMA believes that there are acceptable options to comply within the existing HIPAA regulations such as reports from investigations. As previously stated, AHIMA is not supportive of routinely providing a copy of an access audit log to patients. Access logs typically contain detailed and granular data. However, AHIMA continues to be concerned that significant resources are required to produce such reports, as the data are not necessarily housed in one central database, nor are they readily available. Covered entities and business associates have complex and diverse organizational structures, and thus it may not be readily apparent who or why specific data were accessed.

Regardless, AHIMA believes that it is essential to review any requested access reports with the patient so that an explanation of the report can be provided.

4. *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?*

AHIMA believes that issues regarding use and disclosure of data are not simply technological issues. Data governance and integrity are critical. AHIMA believes that the top priority for patients is the issue of trust. Patients need to trust that their healthcare providers are complying with all relevant and applicable federal and state laws related to the confidentiality, privacy, and security of their health information. AHIMA believes that patients seek assurances that their data are protected from unauthorized use or disclosure.

> *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?*

AHIMA believes that providers should continue to follow their policies and procedures for investigating potential breaches and reporting confirmed breaches as required by Breach Notification Rule. AHIMA is aware of efforts to establish principles of data stewardship and governance, [2] [3] [4] and stands ready to help further refine and evaluate these efforts.

AHIMA believes that in accordance with HIPAA, providers have already implemented processes to ensure that information is only being accessed for legitimate reasons.

Organizations responsible for PHI should already have clearly defined policies and procedures for the access and disclosure of health information. In addition, organizations should have training and monitoring programs in place to enforce compliance.

When inappropriate access or disclosures are identified, providers typically take appropriate steps to counsel their workforce, up to and including termination. Security measures are established to ensure that only caregivers who are participating in the care of a patient or staff working within scope of their jobs have access to a patient's record. In addition, role management is often implemented to limit access to those who have a legitimate need to know. Finally, facilities are required to comply with all federal and state laws associated with privacy and security and educate and re-educate all workforce members on these policies and practices.

In addition, if patients are not satisfied, they may file a complaint with the Privacy Officer or the Office for Civil Rights.

[2] "Health Data Stewardship: What, Why, Who, How An NCVHS Primer." September 2009. http://www.ncvhs.hhs.gov/090930lt.pdf.

[3] Bloomrosen, M., and D. Detmer. "Advancing the Framework: Use of Health Data--A Report of a Working Conference of the American Medical Informatics Association." *Journal of the American Medical Informatics Association* 15, no. 6 (2008): 715-22.

[4] Safran, C., M. Bloomrosen, W.E. Hammond, S. Labkoff, S. Markel-Fox, P.C. Tang, and D.E. Detmer. "Toward a National Framework for the Secondary Use of Health Data: An American Medical Informatics Association White Paper." *Journal of the American Medical Informatics Association* 14, no. 1 (2007): 1-9.

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?*

AHIMA believes that in general organizations are currently successfully addressing accounting for disclosures to external parties. As patient records continue to move to electronic environments, AHIMA recommends that covered entities and business associates coordinate and centralize their release of information functions, especially accounting of disclosures, within an organization's health information management processes.

AHIMA understands that in some settings, the release of information process may be more loosely defined and may require additional attention. Internal access by staff and practitioners may not be routinely or easily tracked. We understand that security audits are used as a primary investigative tool. Telephone lines or support lines, also known as "hotlines," are available to allow organization staff to report irregular or suspicious activities.

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?*

AHIMA members report that tracking each user who accesses a record internally along with the purpose of that access, would be extremely cumbersome and burdensome for all healthcare organizations. We are concerned that current technological solutions and related workflow processes may not be able to consistently and efficiently identify internal user access.

AHIMA believes that the HIPAA Security Rule already requires that organizations be able to track of user access. These capabilities are, however, costly in both financial and human resources. In addition, the data is expansive because of the increasingly larger number of individuals involved in various aspects of the healthcare delivery process that across multiple organizational entities and delivery systems.

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?*

AHIMA believes that the availability to electronically utilize "user roles" or other mechanisms to appropriately distinguish the various types of accesses or disclosures varies widely by organization and by electronic system.

While policies and practices vary from organization to organization, generally, individuals who are not employed, or granted privileges to practice at a given organization, do not have access to patient information within that organization.

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?*

AHIMA is not aware of whether specific vendor technology has the capability to track access, use, or disclosure by vendor employees. However, we remind the Tiger Team that the privacy and security of the data is generally covered by contract between the two parties. Under HIPAA, business associates are bound by the privacy and security policies of both the organization they are working with and their own policies and procedures. Our understanding is that if a vendor logs into a system, the audit trail has the capability to track if the vendor viewed, printed, or edited any information while in the system if they accessed a record.

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?*

According to our members, patients do not seem concerned about general access by staff performing their job duties. For example, patients understand that allied health professionals such as therapists and pharmacists need to access records to know what has been ordered for the patient.

AHIMA questions the extent to which currently available technologies can automatically and accurately discern appropriate uses/access from inappropriate uses/access. We believe that significant human interaction/judgment is required. Furthermore, organizational policies and procedures that govern data access, use, integrity, and governance must be in place and providers and employees must be regularly trained.

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?*

AHIMA members report that some systems can generate some reports. The reports are cumbersome and difficult to generate.

- *How frequently are the reports generated, and what do they look like?*

Typically reports are usually generated from audits or when there is a patient complaint. Report formats vary.

- *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?*

The granularity of the reports varies.

- *Can they be generated automatically, or do you use manual processes?*

Manual processes are usually required.

- *Do you integrate reports across multiple systems?*

Typically reports cannot be generated across multiple systems.

- *What is the look-back period?*

The look-back period varies based on the system's capability.

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?*

Our members report that these requests are very infrequent. When patients make such requests, our members typically ask patients to be as specific as possible regarding their concerns about who might have inappropriately accessed their information. Reviewing an extensive report of internal access to ensure that all access was appropriate is labor intensive, since doing so requires researching every user ID on the list, matching that user ID to a name, and then investigating the purpose of the access.

Members have also shared that providing the actual access report raises more questions and concerns from the patient, such as confirming why the access was appropriate for the individual's job duties. Our members report instances of patients confronting or contacting staff directly if individuals are identified by first and last name on the report.

2. *What types of record use/access/disclosure transparency or tracking technologies are you deploying now and how are you using them?*

AHIMA members stated that they are generally using accounting of disclosure applications supplied by their vendors or still use a paper/manual process. The application is used to track external requests for records and internal requests. AHIMA members also note that not all requests for information or for disclosures of access are handled by the organization's health information management function/department (such as birth and or death certificates reporting or specific diseases that are reported to a state department of health).

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?*

The offer to investigate potential concerns regarding the access, use, or disclosure of PHI and then discussing the results of the investigation or sending a summary letter appears to meet patient needs. Employee names are generally not provided and AHIMA would not support making them available.

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?*

Our members are not aware of any widely mechanisms by which patients can request limits on access. Access management tools appear to be the primary means used to control access to patient records. However, the ability to employ access management as a solution depends upon system configuration.

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?*

Our respondents indicated that nothing beyond the basic information is collected.

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?*

Reviewing access information from business associates would need to be negotiated into the business associate contract. If the covered entity does not currently have review or audit ability written into the contract then that function/process would need to be added.

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?*

This raises major employee safety concerns. AHIMA is very concerned about protecting the staff of the covered entity. Healthcare workers should expect to be safe in their workplace. AHIMA believes that identifying individuals in an access report would unnecessarily jeopardize that safety. We can think of no other industry that places employees in this type of predicament. Further, we are not aware of any other industry that is required to share its internal uses of data with the consumer. This data comprises the business records of the covered entity or business associate. AHIMA believes that any type of access report should only carry identifiers for the workforce members who appear on the report, not individual names. Identifiers would make workforce members more difficult to identify and help to enhance their safety. One option might be to emulate the common practice of using only employee first names and last name initials on an ID badge.

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?*

AHIMA believes current mechanisms to allow patients to file a complaint and request an investigation regarding possible inappropriate uses or disclosures are working. Patients know they can file a complaint and that it will be investigated. Patients are also made aware and provided information to file a complaint with the Secretary if they so choose. Extensive manual processes are required to compile and interpret an access report as part of any investigation. A contributing factor to the work involved is the current lack of a standard format for an access report or log. Standardizing the access reports has the potential to lessen the time and labor it takes to conduct an investigation.

As stated in our July 29, 2011, submitted comments regarding the Accounting of Disclosures Notice of Proposed Rulemaking (NPRM), "AHIMA believes that education is necessary prior to implementation of the rule to ensure that individuals fully understand the various types of accesses that can be included on an access report. And we re-affirmed that AHIMA fully supports the individual's right to understand what to expect when he or she receives an access report. "[5] Furthermore, AHIMA believes that there is a need to educate patients about the definitional differences between the *use* (***means, with respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information)***[6] and the *disclosure* (***means the release, transfer, provision of access to, or divulging in any manner of information outside the entity holding the information)***[7] of PHI. These terms are often used synonymously and that creates challenges with regard to the proper use of PHI for treatment, payment and healthcare operations.

- *Should entities be required to do such an investigation – if so, what should be the scope?*

AHIMA supports the investigation of suspected inappropriate use or disclosure of PHI. Complaint investigations are part of the Breach Notification Rule and should be part of the mitigation process. We also believe that any processes or investigations required to providing responses to such access and use questions must be tempered with a balance

[5] Rode, Dan. "AHIMA Comments on HIPAA Privacy Rule Accounting of Disclosures." July 29, 2011. Available at http://www.ahima.org.

[6] HIPAA Administrative Simplification Regulation Text. March 2013. http://www.hhs.gov/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf.

[7] HIPAA Administrative Simplification Regulation Text. March 2013. http://www.hhs.gov/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf.

that includes an emphasis on the burden and value of the response and the safety of the healthcare workforce involved.

- *Should entities still be required to produce a report if the patient wants one?*

Employee safety concerns are paramount. Patients should have the right to file a complaint regarding potential inappropriate access to or disclosure from their records, as it exists now. The covered entity should then respond by conducting an investigation according to its organizational policies and procedures in compliance with the existing Breach Notification Rules.

Patients should be required to identify [to the best of their ability] the individuals (by name) who they think may have inappropriately accessed their records. Then standard investigation procedures to address the concern would follow.

What recourse does the patient have if he/she is not satisfied with the response?

The privacy rule requires that organizations provide patients with the information to file a complaint with the HHS Office for Civil Rights.

What options do entities have if patient's transparency requests cannot be honored?

AHIMA is not sure what is meant by a “patient's transparency request.” However, we believe that covered entities can only be held accountable for the maintenance of records in accordance with state law regarding health record retention and destruction.

Additionally, AHIMA is concerned about any proposal to inform a patient about any disciplinary actions taken against specific employees. There are specific human resources rules and labor laws that prohibit informing other employees about specific employee sanctions. It would not be appropriate to share that information with patients. It would be appropriate to inform the patient that the situation has been addressed without including any specifics.

Conclusion

Thank you for providing AHIMA the opportunity to testify today. As an addendum to our testimony, AHIMA is supplying the Tiger Team with several additional resources:

- AHIMA Comments on the Accounting of Disclosures Notice of Proposed Rulemaking
- AHIMA Release of Information Toolkit

We look forward to working with key stakeholders to identify proper balance of an individual's request and an appropriate process for accounting of disclosures to ensure the safety of our healthcare workforce.